

Referentenentwurf

des Bundesministeriums des Innern

Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit

A. Problem und Ziel

Polizei- und Strafverfolgungsbehörden müssen zum Schutz der inneren Sicherheit auf neue Herausforderungen reagieren können. Im vergangenen Jahr kam es im öffentlichen Raum vermehrt zu schweren Gewalttaten durch Einzeltäter wie in Mannheim, Solingen, Magdeburg, Aschaffenburg und Hamburg. Es besteht eine hohe abstrakte Bedrohungslage für die Sicherheit in Deutschland – auch durch den internationalen Terrorismus. Erhebliche Bedrohungen gehen ebenso von der schweren und organisierten Kriminalität aus; das zeigt sich unter anderem an der gestiegenen Gewaltbereitschaft sowie am zunehmenden Unterwanderungspotential krimineller Gruppierungen in gesellschaftlichen Strukturen.

Die Bedrohung durch terroristische und kriminelle Strukturen erfordert den Einsatz technologischer Instrumente – auch Künstlicher Intelligenz – in der Gefahrenabwehr und der Strafverfolgung. Ziel des Gesetzentwurfs ist es, den Polizeibehörden die rechtlichen Befugnisse zur Verfügung zu stellen, um den Herausforderungen sachgerecht begegnen zu können.

B. Lösung

Der Gesetzentwurf enthält Befugnisse zur automatisierten Datenanalyse, für den biometrischen Internetabgleich sowie das Testen und Trainieren von IT-Produkten für die Polizeibehörden des Bundes, sowohl für die Gefahrenabwehr als auch die Strafverfolgung. Dieser Gesetzentwurf bildet mit dem Entwurf eines Gesetzes zur Stärkung der Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus ein Gesetzespaket. Er enthält die zustimmungsfreien Bestandteile des Pakets.

Der Gesetzentwurf umfasst Befugnisse für Bundeskriminalamt und Bundespolizei im Rahmen der bestehenden polizeilichen Aufgaben. Von hervorgehobener Bedeutung sind die Befugnisse im Rahmen der Aufgabe des Bundeskriminalamts als Zentralstelle. Zudem erfolgt eine Angleichung der Regelung zum biometrischen Internetabgleich im Asylgesetz an die gegenständlichen Vorschriften.

Die automatisierte Datenanalyse ist ein zentraler Baustein, um die stetig wachsenden Datenmengen in polizeilichen Gefahrenabwehr- und Ermittlungsverfahren verarbeiten zu können. Mittels der Analyse bereits rechtmäßig erhobener polizeilicher Daten ist es möglich, Verbindungen zwischen Taten, Personen, Orten sowie an deren Anknüpfungspunkten zu finden. Insbesondere für komplexe Ermittlungen in den Bereichen Terrorismus, schwerer und organisierter Kriminalität, ist die automatisierte Datenanalyse als Ermittlungsinstrument notwendig. Überdies ermöglicht sie es, in konkreten Anschlagssituationen schnellstmöglich Daten auszuwerten und somit weitere Maßnahmen zur Gefahrenabwehr zu ergreifen.

Der biometrische Abgleich mit öffentlich zugänglichen Daten aus dem Internet ist erforderlich, um Personen insbesondere zu identifizieren, lokalisieren sowie Tat-Täter-Zusammenhänge zu erschließen. Die Befugnis erlaubt es, biometrische Daten – zum Beispiel das Lichtbild einer gesuchten Person – mit öffentlich zugänglichen Daten aus dem Internet

abzugleichen. Im Rahmen der Ausübung der Befugnis ist die Zusammenarbeit mit Dritten, auch außerhalb der Europäischen Union, erlaubt.

IT-Produkte sind elementarer Bestandteil einer modernen polizeilichen Arbeit. Der Gesetzesentwurf enthält eine Befugnis für das Testen und Trainieren von IT-Produkten. Dies umfasst auch selbstlernende Systeme.

Die Befugnisse sind technik- und produktneutral ausgestaltet.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Ergänzung erfolgt im Rahmen der Ressortabstimmung.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entsteht kein Erfüllungsaufwand.

Davon Bürokratiekosten aus Informationspflichten

Keine.

E.3 Erfüllungsaufwand der Verwaltung

Ergänzung erfolgt im Rahmen der Ressortabstimmung.

F. Weitere Kosten

Es entstehen keine weiteren Kosten.

Referentenentwurf des Bundesministeriums des Innern

Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des Bundeskriminalamtgesetzes

Das Bundeskriminalamtgesetz vom 1. Juni 2017 (BGBl. I S. 1354; 2019 I S. 400), das zuletzt durch [...] geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

a) Nach der Angabe zu § 9 werden die folgenden Angaben eingefügt:

„§ 9a Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

§ 9b Automatisierte Datenanalyse“.

b) Die Angabe zu § 22 wird durch die folgende Angabe ersetzt:

„§ 22 Weiterverarbeitung von Daten zu weiteren Zwecken“.

c) Nach der Angabe zu § 63a werden die folgenden Angaben eingefügt:

„§ 63b Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

§ 63c Automatisierte Datenanalyse“.

2. Nach § 9 werden die folgenden §§ 9a, 9b eingefügt:

„§ 9a

Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

(1) Das Bundeskriminalamt kann öffentlich zugängliche personenbezogene Daten, die biometrische Merkmale enthalten, aus dem Internet erheben und mit Daten, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgleichen, sofern

1. bestimmte Tatsachen den Verdacht begründen, dass eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat begangen worden ist oder bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine solche Straftat begehen wird,

2. dies zur Ergänzung vorhandener Sachverhalte zum Zweck der Identifizierung, Aufenthaltsermittlung, Erforschung des Sachverhalts oder Ermittlung von Zusammenhängen mit anderen Straftaten oder Gefahren im Rahmen der Erfüllung seiner Aufgabe als Zentralstelle nach § 2 Absatz 2 Nummer 1 erforderlich ist, und
3. die Verfolgung oder Verhütung der Straftat auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Ein Abgleich mit öffentlich zugänglichen Echtzeitdaten ist unzulässig.

(2) Die Maßnahme nach Absatz 1 Satz 1 darf durchgeführt werden

1. gegen Tatverdächtige, Beschuldigte und nach Gefahrenabwehrrecht entsprechend § 18 oder § 19 des Bundespolizeigesetzes polizeipflichtige Personen sowie Personen nach § 18 Absatz 1 Nummer 4 und
2. gegen Personen nach § 19 Absatz 1 Satz 1 sowie nach Gefahrenabwehrrecht entsprechend § 21 des Bundespolizeigesetzes polizeipflichtige Personen, sofern dies dem Zweck der Identifizierung oder Aufenthaltsermittlung dient, und überwiegende schutzwürdige Interessen dieser Personen nicht entgegenstehen.

(3) Für die nach Absatz 1 Satz 1 abzugleichenden Daten ist § 12 Absatz 2 anzuwenden. Der Abgleich mit Daten, die aus in § 12 Absatz 3 genannten Maßnahmen erlangt wurden, ist unzulässig.

(4) Die im Rahmen des biometrischen Abgleichs nach Absatz 1 Satz 1 erhobenen und verarbeiteten Daten sind nach dessen Durchführung unverzüglich zu löschen, sofern sie keinen konkreten Ermittlungsansatz für den Ausgangssachverhalt aufweisen. Durch organisatorische und technische Maßnahmen hat das Bundeskriminalamt zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind. Für die Protokollierung der Verarbeitungsschritte gilt § 82 Absatz 1. Zudem ist die Zielperson zu protokollieren.

(5) Das Bundeskriminalamt kann den Abgleich durch eine inländische öffentliche oder nichtöffentliche Stelle oder eine öffentliche oder nichtöffentliche Stelle eines Mitgliedsstaats der Europäischen Union durchführen lassen, hierzu an diese Stelle erforderliche Daten übermitteln und, sofern erforderlich, und von § 25 Absatz 6, auch in Verbindung mit § 26, abweichen, wenn

1. die Voraussetzungen des Absatzes 1 Satz 1 erfüllt sind und
2. der Abgleich durch das Bundeskriminalamt selbst technisch unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich ist.

(6) Das Bundeskriminalamt kann den Abgleich durch eine öffentliche und nichtöffentliche Stelle in einem Drittstaat durchführen lassen und hierzu an diese Stelle erforderliche Daten übermitteln, wenn

1. dies zum Zweck des Schutzes der nationalen Sicherheit erforderlich ist,
2. die Voraussetzungen des Absatzes 1 Satz 1 sowie vorbehaltlich des Satzes 2 die Voraussetzungen des § 27 Absatz 8 und des § 81 des Bundesdatenschutzgesetzes erfüllt sind und
3. der Abgleich durch das Bundeskriminalamt selbst oder eine inländische öffentliche oder nichtöffentliche Stelle oder eine öffentliche oder nichtöffentliche Stelle eines

Mitgliedsstaats der Europäischen Union technisch unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich ist.

Sofern dies erforderlich ist, darf das Bundeskriminalamt von § 81 Absatz 1 Nummer 3 und Absatz 4 des Bundesdatenschutzgesetzes abweichen.

(7) Die §§ 25 bis 28 bleiben im Übrigen unberührt.

(8) Die Maßnahme nach Absatz 6 darf nur auf Antrag der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung durch die Präsidentin oder den Präsidenten des Bundeskriminalamtes oder ihre oder seine Vertretung getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit die Anordnung nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft. Die Präsidentin oder der Präsident des Bundeskriminalamtes kann die Antragsbefugnis nach Satz 1 sowie die Anordnungsbefugnis nach Satz 2 auf Bedienstete des Bundeskriminalamtes mit Befähigung zum Richteramt übertragen.

§ 9b

Automatisierte Datenanalyse

(1) Das Bundeskriminalamt kann zur Erfüllung der Aufgabe als Zentralstelle Daten, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, nach Maßgabe von § 12 mittels einer automatisierten Anwendung zur Datenverarbeitung zusammenführen und darüber hinaus zum Zwecke der Analyse weiterverarbeiten, sofern bestimmte Tatsachen

1. den Verdacht begründen, dass eine Straftat im Sinne des § 100a Absatz 2 der Strafprozessordnung begangen worden ist, die Tat auch im Einzelfall schwer wiegt, und dies zur Verfolgung der Straftat erforderlich ist, oder
2. die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat begehen wird, die in § 100a Absatz 2 der Strafprozessordnung genannt ist und sich gegen den Bestand oder die Sicherheit des Bundes oder eines Landes oder gegen Leib, Leben oder Freiheit einer Person oder gegen Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, richtet, und dies zur Verhütung der Straftat erforderlich ist.

(2) Die Maßnahme nach Absatz 1 darf durchgeführt werden gegen

1. Tatverdächtige, Beschuldigte oder nach Gefahrenabwehrrecht entsprechend § 18 oder § 19 des Bundespolizeigesetzes polizeipflichtige Personen sowie Personen nach § 18 Absatz 1 Nummer 4 und
2. Personen nach § 19 Absatz 1 Satz 1 sowie nach Gefahrenabwehrrecht entsprechend § 21 des Bundespolizeigesetzes polizeipflichtige Personen, sofern überwiegende schutzwürdige Interessen dieser Personen nicht entgegenstehen.

(3) Eine direkte Anbindung der Anwendung zur automatisierten Datenanalyse an Register, die nicht in den Anwendungsbereich der Richtlinie (EU) 2016/680 fallen, und an Internetdienste ist unzulässig. Datensätze aus gezielten, auch automatisierten Abfragen in sonstigen staatlichen Registern und im Einzelfall erhobene Datensätze aus Internetquellen können in die Weiterverarbeitung einbezogen werden.

(4) Im Rahmen der Weiterverarbeitung nach Absatz 1 können

1. datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Verfahren, Vorgängen, Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen identifiziert und hergestellt werden, sowohl qualitativ als auch quantitativ klassifiziert, strukturell analysiert und visualisiert werden,
2. für die Erreichung des Zwecks der Weiterverarbeitung nach Absatz 1 unbedeutende Informationen und Erkenntnisse ausgeschlossen werden,
3. die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet werden,
4. Suchkriterien, insbesondere nach Sachnähe, Aktualität und Erheblichkeit der Verknüpfung mit anderen Informationen bezogen auf den Zweck der Weiterverarbeitung nach Absatz 1, gewichtet werden, sowie
5. gespeicherte Daten statistisch ausgewertet werden.

(5) Das Bundeskriminalamt hat bei der Weiterverarbeitung nach Absatz 1 sicherzustellen, dass diskriminierende Algorithmen weder hausgebildet noch verwendet werden. Die § 12, § 22 Absatz 2 sowie Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung bleiben unberührt. Eine ausschließlich auf der Maßnahme nach Absatz 1 beruhende automatisierte Entscheidungsfindung, die unmittelbar eine nachteilige Rechtsfolge für die betroffene Person hat oder diese erheblich beeinträchtigt, ist unzulässig.

(6) Das Bundeskriminalamt gewährleistet im Rahmen der Regelung der Zugriffsberechtigungen nach § 15, dass das für die Durchführung der Maßnahme nach Absatz 1 eingesetzte Personal besonders geschult wird. Durch organisatorische und technische Maßnahmen hat das Bundeskriminalamt zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind. Für die Protokollierung der Zugriffe und Verarbeitungsschritte gilt § 82 Absatz 1. Zudem ist die Zielperson zu protokollieren. Die Übermittlung von personenbezogenen Daten an andere Stellen zur Durchführung der automatisierten Datenanalyse nach Absatz 1 ist unzulässig.

(7) Die Maßnahme nach Absatz 1 ist durch die Präsidentin oder den Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung oder durch eine Bedienstete oder einen Bediensteten des Bundeskriminalamts mit Befähigung zum Richteramt anzuordnen.“

3. § 22 wird wie folgt geändert:

- a) Die Überschrift wird durch die folgende Überschrift ersetzt:

„§ 22

Weiterverarbeitung von Daten zu weiteren Zwecken“.

- b) Nach Absatz 2 werden die folgenden Absätze 3 und 4 eingefügt:

„(3) Das Bundeskriminalamt darf bei ihm vorhandene personenbezogene Daten zur Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten einschließlich selbstlernender Systeme weiterverarbeiten, sofern dies zur Erfüllung seiner Aufgaben erforderlich ist, insbesondere weil

1. unveränderte Daten benötigt werden oder
2. eine Anonymisierung oder Pseudonymisierung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Das Trainieren von IT-Produkten mit personenbezogenen Daten, die aus in § 12 Absatz 3 genannten Maßnahmen erlangt wurden, ist unzulässig. Durch organisatorische und technische Maßnahmen hat das Bundeskriminalamt zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(4) Unter den Voraussetzungen von Absatz 3 darf das Bundeskriminalamt, sofern dies zur Erfüllung seiner Aufgaben erforderlich ist, bei ihm vorhandene personenbezogene Daten an inländische öffentliche oder nichtöffentliche Stellen, Stellen nach § 26 Absatz 1 Satz 1 Nummer 1 und 2, Absatz 2 sowie Stellen nach § 27 Absatz 1 Satz 1 übermitteln. § 28 bleibt unberührt. Eine Übermittlung von Daten nach § 12 Absatz 3 ist unzulässig. Personenbezogene Daten werden nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absatz 2, 3 und 4 Nummer 2 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Der Empfänger darf die übermittelten Daten nur zu dem Zweck nach Absatz 3 weiterverarbeiten. Das Bundeskriminalamt hat die empfangene Stelle darauf hinzuweisen. Absatz 3 Satz 3 gilt entsprechend.“

4. Nach § 63a werden die folgenden §§ 63b, 63c eingefügt:

„§ 63b

Automatisierter biometrischer Abgleich mit öffentlich verfügbaren Daten aus dem Internet

(1) Das Bundeskriminalamt kann öffentlich zugängliche personenbezogene Daten, die biometrische Merkmale enthalten, aus dem Internet erheben und mit Daten, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgleichen, sofern dies im Einzelfall zum Zweck der Identifizierung, Aufenthaltsermittlung, Erforschung des Sachverhalts oder Ermittlung von Zusammenhängen von Straftaten oder Gefahren erforderlich ist

1. zur Abwehr einer Gefahr für eine zu schützende Person oder für eine zu schützende Räumlichkeit nach § 6 oder
2. zum Schutz von Leib, Leben, Freiheit, sexueller Selbstbestimmung oder bedeutenden Sachwerten einer zu schützenden Person oder zum Schutz einer zu schützenden Räumlichkeit nach § 6, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, an dem bestimmte Personen beteiligt sein werden, oder
3. zum Schutz von Leib, Leben, Freiheit oder sexueller Selbstbestimmung einer zu schützenden Person oder zum Schutz einer zu schützenden Räumlichkeit nach § 6, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in einem übersehbaren Zeitraum eine Straftat gegen eines dieser Rechtsgüter der zu schützenden Person oder gegen eine zu schützende Räumlichkeit begehen wird,

und die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre. Ein Abgleich mit öffentlich zugänglichen Echtzeitdaten ist unzulässig.

(2) Die Maßnahme nach Absatz 1 Satz 1 darf durchgeführt werden

1. gegen die entsprechend § 18 oder § 19 des Bundespolizeigesetzes Verantwortlichen oder Personen im Sinne von Absatz 1 Nummer 2 oder 3 und
2. gegen Personen entsprechend § 21 des Bundespolizeigesetzes, sofern überwiegende schutzwürdige Interessen dieser Personen nicht entgegenstehen.

(3) Für die nach Absatz 1 Satz 1 abzugleichenden Daten ist § 12 Absatz 2 anzuwenden. Der Abgleich mit Daten, die die aus in § 12 Absatz 3 genannten Maßnahmen erlangt wurden, ist unzulässig.

(4) Die im Rahmen des biometrischen Abgleichs nach Absatz 1 Satz 1 erhobenen und verarbeiteten Daten sind nach dessen Durchführung unverzüglich zu löschen, sofern sie keinen konkreten Ermittlungsansatz für den Ausgangssachverhalt aufweisen. Durch organisatorische und technische Maßnahmen hat das Bundeskriminalamt zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind. Für die Protokollierung der Verarbeitungsschritte gilt § 82 Absatz 1. Zudem ist die Zielperson zu protokollieren.

(5) Das Bundeskriminalamt kann den Abgleich durch eine inländische öffentliche oder nichtöffentliche Stelle oder eine öffentliche oder nichtöffentliche Stelle eines Mitgliedsstaats der Europäischen Union durchführen lassen, hierzu an diese Stelle erforderliche Daten übermitteln und, sofern erforderlich, von § 25 Absatz 6, auch in Verbindung mit § 26, abweichen, wenn

1. die Voraussetzungen des Absatzes 1 Satz 1 erfüllt sind und
2. der Abgleich durch das Bundeskriminalamt selbst technisch unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich ist.

(6) Das Bundeskriminalamt kann den Abgleich durch eine öffentliche oder nichtöffentliche Stelle in einem Drittstaat durchführen lassen und hierzu an diese Stelle erforderliche Daten übermitteln, wenn

1. dies zum Zweck des Schutzes der nationalen Sicherheit erforderlich ist,
2. die Voraussetzungen des Absatzes 1 Satz 1 sowie vorbehaltlich des Satzes 2 die Voraussetzungen des § 27 Absatz 8 und des § 81 des Bundesdatenschutzgesetzes erfüllt sind und
3. der Abgleich durch das Bundeskriminalamt selbst oder eine inländische öffentliche oder nichtöffentliche Stelle oder eine öffentliche oder nichtöffentliche Stelle eines Mitgliedsstaats der Europäischen Union technisch unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich ist.

Sofern dies erforderlich ist, darf das Bundeskriminalamt von § 81 Absatz 1 Nummer 3 und Absatz 4 des Bundesdatenschutzgesetzes abweichen.

(7) Die §§ 25 bis 28 bleiben im Übrigen unberührt.

(8) Die Maßnahme nach Absatz 6 darf nur auf Antrag der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung durch die

Präsidentin oder den Präsidenten des Bundeskriminalamtes oder ihre oder seine Vertretung getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit die Anordnung nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft. Die Präsidentin oder der Präsident des Bundeskriminalamtes kann die Antragsbefugnis nach Satz 1 sowie die Anordnungsbefugnis nach Satz 2 auf Bedienstete des Bundeskriminalamtes mit Befähigung zum Richteramt übertragen.

§ 63c

Automatisierte Datenanalyse

(1) Das Bundeskriminalamt kann Daten, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, nach Maßgabe von § 12 mittels einer automatisierten Anwendung zur Datenverarbeitung zusammenführen und darüber hinaus zum Zwecke der Analyse weiterverarbeiten, sofern dies zur Abwehr einer im Einzelfall bestehenden Gefahr für Leib, Leben oder Freiheit einer nach § 6 zu schützenden Person erforderlich ist. Eine Maßnahme nach Satz 1 ist auch zulässig, sofern

1. Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat von auch im Einzelfall erheblicher Bedeutung gegen Leib, Leben oder Freiheit einer nach § 6 zu schützenden Person begehen wird, oder
2. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine Straftat von auch im Einzelfall erheblicher Bedeutung gegen Leib, Leben oder Freiheit einer nach § 6 zu schützenden Person begehen wird,

und dies zur Verhütung dieser Straftat erforderlich ist.

(2) Die Maßnahme nach Absatz 1 darf durchgeführt werden gegen

1. die entsprechend § 18 oder § 19 des Bundespolizeigesetzes Verantwortlichen oder Personen im Sinne von Absatz 1 Satz 2 Nummer 1 oder 2 und
2. Personen entsprechend § 21 des Bundespolizeigesetzes, sofern überwiegende schutzwürdige Interessen dieser Personen nicht entgegenstehen.

(3) Eine direkte Anbindung der Anwendung zur automatisierten Datenanalyse an Register, die nicht in den Anwendungsbereich der Richtlinie (EU) 2016/680 fallen, und an Internetdienste ist unzulässig. Datensätze aus gezielten, auch automatisierten Abfragen in sonstigen staatlichen Registern und im Einzelfall erhobene Datensätze aus Internetquellen können in die Weiterverarbeitung einbezogen werden.

(4) Im Rahmen der Weiterverarbeitung nach Absatz 1 Satz 1 können

1. datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Verfahren, Vorgängen, Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen identifiziert und hergestellt werden, sowohl qualitativ als auch quantitativ klassifiziert, strukturell analysiert und visualisiert werden,
2. für die Erreichung des Zwecks des Weiterverarbeitung nach Absatz 1 unbedeutende Informationen und Erkenntnisse ausgeschlossen werden,
3. die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet werden,

4. Suchkriterien, insbesondere nach Sachnähe, Aktualität und Erheblichkeit der Verknüpfung mit anderen Informationen bezogen auf den Zweck der Weiterverarbeitung nach Absatz 1, gewichtet werden, sowie
5. gespeicherte Daten statistisch ausgewertet werden.

(5) Das Bundeskriminalamt hat bei der Weiterverarbeitung nach Absatz 1 sicherzustellen, dass diskriminierende Algorithmen weder hausgebildet noch verwendet werden. Die § 12, § 22 Absatz 2 sowie Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung bleiben unberührt. Eine ausschließlich auf der Maßnahme nach Absatz 1 beruhende automatisierte Entscheidungsfindung, die unmittelbar eine nachteilige Rechtsfolge für die betroffene Person hat oder diese erheblich beeinträchtigt, ist unzulässig.

(6) Das Bundeskriminalamt gewährleistet im Rahmen der Regelung der Zugriffsberechtigungen nach § 15, dass das für die Durchführung der Maßnahme nach Absatz 1 eingesetzte Personal besonders geschult wird. Durch organisatorische und technische Maßnahmen hat das Bundeskriminalamt zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind. Für die Protokollierung der Zugriffe und Verarbeitungsschritte gilt § 82 Absatz 1. Zudem ist die Zielperson zu protokollieren. Die Übermittlung von personenbezogenen Daten an andere Stellen zur Durchführung der automatisierten Datenanalyse nach Absatz 1 ist unzulässig.

(7) Die Maßnahme nach Absatz 1 ist durch die Präsidentin oder den Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung oder durch eine Bedienstete oder einen Bediensteten des Bundeskriminalamts mit Befähigung zum Richteramt anzuordnen.“

Artikel 2

Änderung des Bundespolizeigesetzes

Das Bundespolizeigesetz vom 19. Oktober 1994 (BGBl. I S. 2978, 2979), das zuletzt durch [...] geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:
 - a) Die Angabe zu § 46 wird durch die folgende Angabe ersetzt:

„§ 46 Weiterverarbeitung von Daten zu weiteren Zwecken“.
 - b) Nach der Angabe zu § 58 die folgenden Angaben eingefügt:

„§ 58a Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

§ 58b Automatisierte Datenanalyse“.
2. § 46 wird wie folgt geändert:
 - a) Die Überschrift wird durch die folgende Überschrift ersetzt:

„§ 46

Weiterverarbeitung von Daten zu weiteren Zwecken“.

b) Nach § 46 Absatz 2 werden die folgenden Absätze 3 und 4 eingefügt:

„(3) Die Bundespolizei kann bei ihr vorhandene personenbezogene Daten zur Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten einschließlich selbstlernender Systeme weiterverarbeiten, sofern dies zur Erfüllung einer ihr obliegenden Aufgabe erforderlich ist, insbesondere weil

1. unveränderte Daten benötigt werden oder
2. eine Anonymisierung oder Pseudonymisierung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Das Trainieren von IT-Produkten mit personenbezogenen Daten, die aus in § 12 Absatz 3 des Bundeskriminalamtgesetzes genannten Maßnahmen erlangt wurden, ist unzulässig. Durch organisatorische und technische Maßnahmen stellt die Bundespolizei sicher, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(4) Unter den Voraussetzungen von Absatz 3 kann die Bundespolizei, sofern dies zur Erfüllung ihrer Aufgaben erforderlich ist, bei ihr vorhandene personenbezogene Daten an inländische öffentliche oder nichtöffentliche Stellen und Stellen nach § 54 Absatz 1 Satz 1 Nummer 1 bis 3 sowie Stellen nach § 56 Absatz 1 Satz 1 übermitteln. § 57 bleibt unberührt. Eine Übermittlung von Daten nach § 12 Absatz 3 des Bundeskriminalamtgesetzes ist unzulässig. Personenbezogene Daten werden nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absatz 2, 3 und 4 Nummer 2 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Der Empfänger darf die übermittelten Daten nur zu dem Zweck nach Absatz 3 weiterverarbeiten. Die Bundespolizei hat die empfangene Stelle darauf hinzuweisen. Absatz 3 Satz 3 gilt entsprechend.“

3. Nach § 58 werden die folgenden §§ 58a, 58b eingefügt:

„§ 58a

Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

(1) Die Bundespolizei kann zur Erfüllung einer ihr obliegenden Aufgabe öffentlich zugängliche personenbezogene Daten, die biometrische Merkmale enthalten, aus dem Internet erheben und mit Daten, auf die sie zur Erfüllung ihrer Aufgaben zugreifen darf, mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgleichen, sofern

1. dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, erforderlich ist,
2. Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine

Straftat im Zusammenhang mit lebensgefährdenden Schleusungen oder eine Straftat, die gegen die Sicherheit der Anlagen oder des Betriebes des Luft-, See- oder Bahnverkehrs gerichtet ist, insbesondere Straftaten nach den §§ 315, 315b, 316b und 316c des Strafgesetzbuches, und eine nicht unerhebliche Schädigung eines der in Nummer 1 genannten Rechtsgüter erwarten lässt, begehen wird, oder

3. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Straftat im Zusammenhang mit lebensgefährdenden Schleusungen oder eine Straftat, die gegen die Sicherheit der Anlagen oder des Betriebes des Luft-, See- oder Bahnverkehrs gerichtet ist, insbesondere Straftaten nach den §§ 315, 315b, 316b und 316c des Strafgesetzbuches, und eine nicht unerhebliche Schädigung eines der in Nummer 1 genannten Rechtsgüter erwarten lässt, begehen wird,

und die Erhebung und der Abgleich im Einzelfall zum Zweck der Identifizierung, Aufenthaltsermittlung, Erforschung des Sachverhalts oder Ermittlung von Zusammenhängen von Straftaten oder Gefahren erforderlich ist und die Abwehr der Gefahr oder die Verhütung der in diesem Absatz genannten Straftaten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Ein Abgleich mit öffentlich zugänglichen Echtzeitdaten ist unzulässig.

(2) Die Maßnahme nach Absatz 1 Satz 1 darf durchgeführt werden

1. gegen die nach § 18 oder § 19 Verantwortlichen oder Personen im Sinne von Absatz 1 Satz 1 Nummer 2 oder 3, und
2. gegen Personen nach § 21, sofern überwiegende schutzwürdige Interessen dieser Person nicht entgegenstehen.

(3) Für die nach Absatz 1 Satz 1 abzugleichenden Daten ist § 43 anzuwenden. Der Abgleich mit Daten, die die aus in § 12 Absatz 3 des Bundeskriminalamtgesetzes genannten Maßnahmen erlangt wurden, ist unzulässig.

(4) Die im Rahmen des biometrischen Abgleichs nach Absatz 1 Satz 1 erhobenen und verarbeiteten Daten sind nach dessen Durchführung unverzüglich zu löschen, sofern sie keinen konkreten Ermittlungsansatz für den Ausgangssachverhalt aufweisen. Die Bundespolizei stellt durch organisatorische und technische Maßnahmen sicher, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(5) Die Bundespolizei kann den Abgleich durch eine inländische öffentliche oder nichtöffentliche Stelle oder eine öffentliche oder nichtöffentliche Stelle eines Mitgliedsstaats der Europäischen Union durchführen lassen, hierzu an diese Stelle erforderliche Daten übermitteln und, sofern erforderlich, von § 53 Absatz 5, auch in Verbindung mit § 54, abweichen, wenn

1. die Voraussetzungen des Absatzes 1 Satz 1 erfüllt sind und
2. der Abgleich durch die Bundespolizei selbst technisch unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich ist.

(6) Die Bundespolizei kann den Abgleich durch eine öffentliche oder nichtöffentliche Stelle in einem Drittstaat durchführen lassen und hierzu an diese Stelle erforderliche Daten übermitteln, wenn

1. dies zum Zweck des Schutzes der nationalen Sicherheit erforderlich ist,

2. die Voraussetzungen des Absatzes 1 Satz 1 sowie vorbehaltlich des Satzes 2 die Voraussetzungen des § 56 Absatz 2 und des § 81 des Bundesdatenschutzgesetzes erfüllt sind und
3. der Abgleich durch die Bundespolizei selbst oder eine inländische öffentliche oder nichtöffentliche Stelle oder eine öffentliche oder nichtöffentliche Stelle eines Mitgliedsstaats der Europäischen Union technisch unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich ist.

Sofern dies erforderlich ist, darf die Bundespolizei von § 81 Absatz 1 Nummer 3 und Absatz 4 des Bundesdatenschutzgesetzes abweichen.

(7) Die §§ 53 bis 57 bleiben im Übrigen unberührt.

(8) Die Maßnahme nach Absatz 6 darf nur auf Antrag der Präsidentin oder des Präsidenten des Bundespolizeipräsidiums oder einer Bundespolizeidirektion, oder ihrer oder seiner Vertretung, durch das Gericht angeordnet werden. Zuständig ist das Amtsgericht, in dessen Bezirk die Behörde der Antragsberechtigten nach Satz 1 ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Buches 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit mit Ausnahme der § 23 Absatz 2, § 37 Absatz 2 und § 41 entsprechend. Die Anordnung ergeht ohne Anhörung der betroffenen Person. Die Anordnung wird mit Erlass wirksam. Bei Gefahr im Verzug kann die Anordnung durch die Präsidentin oder den Präsidenten des Bundespolizeipräsidiums oder einer Bundespolizeidirektion, oder ihre oder seine Vertretung, getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit die Anordnung nach Satz 6 nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

§ 58b

Automatisierte Datenanalyse

(1) Die Bundespolizei kann zur Erfüllung einer ihr obliegenden Aufgabe Daten, auf die sie zur Erfüllung ihrer Aufgaben zugreifen darf, nach Maßgabe von § 43 mittels einer automatisierten Anwendung zur Datenverarbeitung zusammenführen und darüber hinaus zum Zwecke der Analyse weiterverarbeiten, sofern

1. dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, erforderlich ist,
2. Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat im Zusammenhang mit lebensgefährdenden Schleusungen oder eine Straftat, die gegen die Sicherheit der Anlagen oder des Betriebes des Luft-, See- oder Bahnverkehrs gerichtet ist, insbesondere Straftaten nach den §§ 315, 315b, 316b und 316c des Strafgesetzbuches, und eine nicht unerhebliche Schädigung eines der in Nummer 1 genannten Rechtsgüter erwarten lässt, begehen wird, und dies zur Abwehr der Gefahr oder zur Verhütung der in diesem Absatz genannten Straftaten erforderlich ist, oder
3. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine Straftat im Zusammenhang mit lebensgefährdenden Schleusungen oder eine Straftat, die gegen die Sicherheit der Anlagen oder des Betriebes des Luft-, See- oder Bahnverkehrs gerichtet ist, insbesondere Straftaten von auch im Einzelfall erheblicher Bedeutung nach den §§ 315, 315b, 316b und 316c des Strafgesetzbuches, und eine nicht

unerhebliche Schädigung eines der in Nummer 1 genannten Rechtsgüter erwarten lässt, begangen wird, und dies zur Abwehr der Gefahr oder zur Verhütung der in diesem Absatz genannten Straftaten erforderlich ist.

(2) Die Maßnahme nach Absatz 1 darf durchgeführt werden gegen

1. die nach § 18 oder § 19 Verantwortlichen oder Personen im Sinne von Absatz 1 Nummer 2 oder 3 und
2. Personen nach § 21, sofern überwiegende schutzwürdige Interessen dieser Person nicht entgegenstehen.

(3) Eine direkte Anbindung der Anwendung zur automatisierten Datenanalyse an Register, die nicht in den Anwendungsbereich der Richtlinie (EU) 2016/680 fallen, und an Internetdienste ist unzulässig. Datensätze aus gezielten, auch automatisierten Abfragen in sonstigen staatlichen Registern und im Einzelfall erhobene Datensätze aus Internetquellen können in die Weiterverarbeitung einbezogen werden.

(4) Im Rahmen der Weiterverarbeitung nach Absatz 1 können

1. datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Verfahren, Vorgängen, Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen identifiziert und hergestellt werden, sowohl qualitativ als auch quantitativ klassifiziert, strukturell analysiert und visualisiert hergestellt werden,
2. für die Erreichung des Zwecks der Weiterverarbeitung nach Absatz 1 unbedeutende Informationen und Erkenntnisse ausgeschlossen werden,
3. die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet werden,
4. Suchkriterien, insbesondere nach Sachnähe, Aktualität und Erheblichkeit der Verknüpfung mit anderen Informationen bezogen auf den Zweck der Weiterverarbeitung nach Absatz 1, gewichtet werden, sowie
5. gespeicherte Daten statistisch ausgewertet werden.

(5) Die Bundespolizei hat bei der Weiterverarbeitung nach Absatz 1 sicherzustellen, dass diskriminierende Algorithmen weder hausgebildet noch verwendet werden. Die § 43, § 46 Absatz 2 sowie Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung bleiben unberührt. Eine ausschließlich auf der Maßnahme nach Absatz 1 beruhende automatisierte Entscheidungsfindung, die unmittelbar eine nachteilige Rechtsfolge für die betroffene Person hat oder diese erheblich beeinträchtigt, ist unzulässig.

(6) Die Bundespolizei gewährleistet im Rahmen der Regelung der Zugriffsberechtigungen, dass das für die Durchführung der Maßnahme nach Absatz 1 eingesetzte Personal besonders geschult wird. Durch organisatorische und technische Maßnahmen stellt sie sicher, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind. Die Übermittlung von personenbezogenen Daten an andere Stellen zur Durchführung der automatisierten Datenanalyse nach Absatz 1 ist unzulässig.

(7) Die Maßnahme nach Absatz 1 darf nur durch die Präsidentin oder den Präsidenten des Bundespolizeipräsidiums oder einer Bundespolizeidirektion, ihrer oder seiner Vertretung oder durch die Leiterin oder den Leiter einer Abteilung des Bundespolizeipräsidiums angeordnet werden.“

4. § 85 wird wie folgt geändert:

a) In Absatz 1 wird die Angabe „und 51“ durch die Angabe „, 51, 58a und 58b“ ersetzt.

b) Absatz 2 wird wie folgt geändert:

aa) In Nummer 7 wird die Angabe „sind.“ durch die Angabe „sind,“ ersetzt.

bb) Nach Nummer 7 wird die folgende Nummer 8 eingefügt:

„8. bei Maßnahmen nach den §§ 58a und 58b die Zielperson.“

Artikel 3

Änderung des Asylgesetzes

Das Asylgesetz in der Fassung der Bekanntmachung vom 2. September 2008 (BGBl. I S. 1798), das zuletzt durch [...] geändert worden ist wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu § 15b durch die folgende Angabe ersetzt:

„§ 15b Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet“.

2. § 15b wird durch den folgenden § 15b ersetzt:

„§ 15b

Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

(1) Das nach § 16 Absatz 1 Satz 1 und 2 erhobene biometrische Lichtbild des Ausländers darf mit öffentlich zugänglichen personenbezogenen Daten, die biometrische Merkmale enthalten, aus dem Internet mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgeglichen werden, wenn der Ausländer keinen gültigen Pass oder Passersatz besitzt und der Abgleich für die Feststellung der Identität oder Staatsangehörigkeit des Ausländers erforderlich ist. Ein Abgleich mit öffentlich zugänglichen Echtzeitdaten ist unzulässig.

(2) Die im Rahmen des Abgleichs nach Absatz 1 erhobenen Daten sind nach Durchführung des Abgleichs unverzüglich zu löschen, sofern sie für die Feststellung der Identität oder Staatsangehörigkeit nicht mehr erforderlich sind. Die Weiterverarbeitung der beim Abgleich erhobenen Daten zu anderen Zwecken ist unzulässig. Der Abgleich, das Ergebnis des Abgleichs und das Löschen von Daten sind in der Asylakte zu dokumentieren.

(3) Durch organisatorische und technische Maßnahmen ist zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind und insbesondere der Herkunftsstaat des Ausländers sowie Drittstaaten, in denen der Ausländer eine Verfolgung oder einen ernsthaften Schaden zu befürchten hat, keine Kenntnis über die Maßnahme nach Absatz 1 Satz 1 erlangen. Bei jeder Maßnahme nach Absatz 1 sind die Bezeichnung der eingesetzten automatisierten Anwendung zur Datenverarbeitung, der Zeitpunkt ihres Einsatzes, die Organisationseinheit und die Person, die die Maßnahme durchführen, zu protokollieren.

(4) Für die in den Absätzen 1 bis 3 genannten Maßnahmen ist das Bundesamt zuständig. Das Bundesamt kann den Abgleich durch eine inländische öffentliche oder nichtöffentliche Stelle oder eine öffentliche oder nichtöffentliche Stelle eines Mitgliedsstaats der Europäischen Union durchführen lassen und hierzu an diese Stelle erforderliche Daten übermitteln, wenn

1. die Voraussetzungen des Absatzes 1 Satz 1 erfüllt sind, und

2. der Abgleich durch das Bundesamt selbst technisch unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich ist.“

Artikel 4

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Polizei- und Strafverfolgungsbehörden müssen zum Schutz der inneren Sicherheit auf neue Herausforderungen reagieren können. Im vergangenen Jahr kam es im öffentlichen Raum vermehrt zu schweren Gewalttaten durch Einzeltäter wie in Mannheim, Solingen, Magdeburg, Aschaffenburg und Hamburg. Es besteht eine hohe abstrakte Bedrohungslage für die Sicherheit in Deutschland – auch durch den internationalen Terrorismus. Erhebliche Bedrohungen gehen ebenso von der schweren und organisierten Kriminalität aus; das zeigt sich unter anderem an der gestiegenen Gewaltbereitschaft sowie am zunehmenden Unterwanderungspotential krimineller Gruppierungen in gesellschaftlichen Strukturen.

Die Bedrohung durch terroristische und kriminelle Strukturen erfordert den Einsatz technologischer Instrumente – auch Künstlicher Intelligenz – in der Gefahrenabwehr und der Strafverfolgung. Ziel des Gesetzentwurfs ist es, den Polizeibehörden die rechtlichen Befugnisse zur Verfügung zu stellen, um den Herausforderungen sachgerecht begegnen zu können.

II. Wesentlicher Inhalt des Entwurfs

Der Gesetzentwurf enthält Befugnisse zur automatisierten Datenanalyse, für den biometrischen Internetabgleich sowie das Testen und Trainieren von IT-Produkten für die Polizeibehörden des Bundes. Dieser Gesetzentwurf bildet mit dem Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus ein Gesetzespaket. Er enthält die zustimmungsfreien Bestandteile des Pakets.

Hinsichtlich des Bundeskriminalamts betrifft dies die Aufgabe als Zentralstelle für die Kriminalpolizei des Bundes und der Länder nach § 2 des Bundeskriminalamtgesetzes (BKAG) sowie den Schutz von Mitgliedern der Verfassungsorgane und der Leitung des Bundeskriminalamts nach § 6 BKAG. Im Hinblick auf die Bundespolizei beziehen sich die Befugnisse auf ihre Aufgabe zur Gefahrenabwehr im Rahmen des Grenzschutzes nach § 2 Absatz 2 Nummer 2 Buchstabe c des Bundespolizeigesetzes (BPolG), auf ihre Aufgabe nach § 3 Absatz 1 BPolG zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung, die auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes den Benutzern, den Anlagen oder dem Betrieb der Bahn drohen, beim Betrieb der Bahn entstehen oder von den Bahnanlagen ausgehen, auf ihre Aufgabe zur Gefahrenabwehr im Bereich der Luftsicherheit nach §§ 4 und 4a BPolG, auf ihre Aufgabe zum Schutz von Bundesorganen nach § 5 BPolG sowie auf ihre Aufgaben auf See nach § 6 BPolG. Zudem erfolgt eine Angleichung der Regelung zum biometrischen Internetabgleich im Asylgesetz an die gegenständlichen Vorschriften.

Die automatisierte Datenanalyse ist ein zentraler Baustein, um die stetig wachsenden Datenmengen in polizeilichen Gefahrenabwehr- und Ermittlungsverfahren verarbeiten zu können. Mittels der Analyse bereits rechtmäßig erhobener polizeilicher Daten ist es möglich, Verbindungen zwischen Taten, Personen, Orten sowie an deren Anknüpfungspunkten zu finden. Insbesondere für komplexe Ermittlungen in den Bereichen Terrorismus, schwerer und organisierter Kriminalität, ist die automatisierte Datenanalyse als Ermittlungsinstrument notwendig. Überdies ermöglicht sie es, in konkreten Anschlagssituationen schnellstmöglich Daten auszuwerten und somit weitere Maßnahmen zur Gefahrenabwehr zu ergreifen.

Der biometrische Abgleich mit öffentlich zugänglichen Daten aus dem Internet ist erforderlich, um Personen insbesondere zu identifizieren, lokalisieren sowie Tat-Täter-Zusammenhänge zu erschließen. Die Befugnis erlaubt es, biometrische Daten – zum Beispiel das Lichtbild einer gesuchten Person – mit öffentlich zugänglichen Daten aus dem Internet abzugleichen. Im Rahmen der Ausübung der Befugnis ist die Zusammenarbeit mit Dritten, auch außerhalb der Europäischen Union, erlaubt.

IT-Produkte sind elementarer Bestandteil einer modernen polizeilichen Arbeit. Der Gesetzentwurf enthält eine Befugnis für das Testen und Trainieren von IT-Produkten. Dies umfasst auch selbstlernende Systeme.

Die Befugnisse sind technik- und produktneutral ausgestaltet.

III. Exekutiver Fußabdruck

Interessenvertreterinnen und Interessenvertreter Dritter oder sonstige Personen außerhalb der Bundesverwaltung sind nicht an der Erstellung des Entwurfs beteiligt worden.

IV. Alternativen

Keine.

V. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt für die Änderung des Bundeskriminalamtgesetzes bezüglich der Zentralstellenfunktion Artikel 73 Absatz 1 Nummer 10 Buchstabe a des Grundgesetzes (GG) und bezüglich des Schutzes von Bundesorganen, Mitgliedern der Verfassungsorgane und der Leitung des Bundeskriminalamts aus der Natur der Sache. Für die Änderungen des Bundespolizeigesetzes folgt die Gesetzgebungskompetenz aus Artikel 73 Absatz 1 Nummer 5 (Grenzschutz), 6 (Luftverkehr) und 6a (Eisenbahnen) GG sowie für die datenschutzrechtlichen Regelungen als Annex zu den jeweiligen Sachkompetenzen. Soweit für die Änderungen des Bundespolizeigesetzes der Schutz von Bundesorganen betroffen ist, folgt die Gesetzgebungskompetenz aus der Natur der Sache. Für die Änderungen des Asylgesetzes folgt die Gesetzgebungskompetenz aus Artikel 74 Absatz 1 Nummer 6 GG.

VI. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland geschlossen hat, vereinbar.

VII. Gesetzesfolgen

Der Gesetzentwurf dient dem Schutz der öffentlichen Sicherheit in Deutschland und der Stärkung der Ermittlungsbefugnisse im Rahmen von Gefahrenabwehr und Strafverfolgung.

1. Rechts- und Verwaltungsvereinfachung

Die Regelungen des Gesetzentwurfs werden nicht zu einer Rechts- oder Verwaltungsvereinfachung führen.

2. Nachhaltigkeitsaspekte

Der Gesetzentwurf steht im Einklang mit den Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Deutschen Nachhaltigkeitsstrategie, die der Umsetzung der Agenda 2030 für nachhaltige Entwicklung der Vereinten Nationen dient. Der Entwurf dient entsprechend der Zielvorgabe 16.1 der Erhöhung der persönlichen Sicherheit und dem Schutz vor Kriminalität.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Ergänzung erfolgt im Rahmen der Ressortabstimmung.

4. Erfüllungsaufwand

a) Erfüllungsaufwand für Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

b) Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entsteht kein Erfüllungsaufwand.

c) Erfüllungsaufwand der Verwaltung

Ergänzung erfolgt im Rahmen der Ressortabstimmung.

5. Weitere Kosten

Weitere Kosten sind nicht zu erwarten.

6. Weitere Gesetzesfolgen

Auswirkungen auf demografierelevante Belange sind nicht zu erwarten.

VIII. Befristung; Evaluierung

Befristung und Evaluierung sind nicht vorgesehen.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Bundeskriminalamtgesetzes)

Zu Nummer 1 (Inhaltsübersicht)

Zu Buchstabe a

Es handelt sich um eine redaktionelle Folgeänderung zur Einführung von den §§ 9a, 9b.

Zu Buchstabe b

Es handelt sich um eine redaktionelle Folgeänderung zur Änderung der Überschrift von § 22.

Zu Buchstabe c

Es handelt sich um eine redaktionelle Folgeänderung zur Einführung von den §§ 63b, 63c.

Zu Nummer 2 (§§ 9a, 9b)

Zu § 9a

Das Bundeskriminalamt hat nach § 2 Absatz 2 Nummer 1 die Aufgabe, alle zur Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung nach § 2 Absatz 1 erforderlichen Informationen zu sammeln und auszuwerten. Als Zentralstelle unterstützt das Bundeskriminalamt die Polizeien des Bundes und der Länder in der gesamten Breite der Kriminalitätsbekämpfung, insbesondere aber in den Feldern der Terrorismusabwehr sowie der schweren und organisierten Kriminalität. Für eine moderne Aufgabenwahrnehmung ist es unerlässlich, dass dies auch Informationen aus dem Internet umfasst. Straftäter hinterlassen in der analogen wie auch digitalen Welt Spuren: Das Bundeskriminalamt muss in beiden Situationen über die erforderlichen Ermittlungsinstrumente verfügen. Diesem Zweck dient § 9a.

Ziel des automatisierten Abgleichs biometrischer Daten mit öffentlich zugänglichen Daten aus dem Internet ist die Identifizierung und Lokalisierung sowie Erkennung von Tat-Täter-Zusammenhängen. Eine entsprechende Befugnis ist neben der hier betroffenen Zentralstellenregelung zur Abwehr von Gefahren des internationalen Terrorismus (§ 39a) und zum Schutz von Mitgliedern der Verfassungsorgane und der Leitung des Bundeskriminalamts (§ 63b) vorgesehen.

Die Befugnis ist technik- und produktneutral. Die Umsetzung kann mittels eigener IT-Produkte des Bundeskriminalamts oder kommerzieller IT-Produkte Dritter erfolgen.

Zu Absatz 1

Ausgangspunkt des Abgleichs nach Absatz 1 Satz 1 ist ein biometrisches Datum, beispielsweise ein Fahndungslichtbild, das mit öffentlich verfügbaren Daten aus dem Internet (Referenzdaten) abgeglichen wird. Dieses Ausgangsdatum kann in der Folge für einen biometrischen Abgleich mit öffentlich verfügbaren Daten, die biometrische Merkmale enthalten, aus dem Internet verwendet werden. Unter einem biometrischen Abgleich im Sinne der Vorschrift ist die technisch gestützte Überprüfung der Übereinstimmung von biometrischen Signaturen mit dem Ergebnis einer Übereinstimmungsbewertung zu verstehen. Unter allgemein öffentlich zugängliche Daten fallen solche Daten, die von jedermann verwendet werden können, beispielsweise aus sozialen Medien, soweit sich diese nicht an einen spezifisch abgegrenzten Personenkreis richten. Konkretisierend fallen darunter Daten, wenn sie jede Person ohne oder nach vorheriger Registrierung, Genehmigung oder Entgeltzahlung nutzen kann. Nicht umfasst sind Daten, die einer spezifischen Schwelle unterzogen sind, beispielsweise der Einstellung von Daten in sozialen Medien für einen begrenzten Kreis, dessen Zugang einer Kontrolle unterzogen wird. Privatkommunikation über Messenger-Dienste von sozialen Medien können nicht von der Maßnahme erfasst werden.

Zweck des Abgleichs ist gemäß Absatz 1 Satz 1 Nummer 1, dass das Bundeskriminalamt zur Erfüllung der Aufgabe nach § 2 Absatz 2 Nummer 1 als Zentralstelle im Bereich der Strafverfolgung und Straftatenverhütung bestehende Hinweise zu Personen und einer bestimmten Begehungsweise verdichten kann. Im Rahmen der Aufgabe nach § 2 Absatz 2 Nummer 1 ist das Bundeskriminalamt verpflichtet, die zur Tätigkeit als Zentralstelle erforderlichen Informationen zu sammeln und auszuwerten. Gemäß § 2 Absatz 1 handelt es sich dabei um die Unterstützung der Polizeien des Bundes oder Länder, die in der Regel die zugrundeliegenden Verfahren führen. Sofern eine Übereinstimmung mit öffentlich verfügbaren Daten aus dem Internet erkannt wird, können dieses Anhaltspunkte für das zugrundeliegende Verfahren liefern. So können durch Lichtbilder Tatverdächtige oder Störer

identifiziert sowie Hinweise auf ihren Aufenthaltsort erhoben werden. Zudem können die erhobenen Daten weitere Hinweise zur Sachverhaltsaufklärung des zugrundeliegenden Verfahrens dienen. Auch für den Zweck der Ermittlung mit anderen Straftaten kann die Befugnis wertvolle Hinweise liefern; so können zum Beispiel Bilder Zusammenhänge mit terroristischen oder kriminellen Gruppierungen oder Symbolen aufzeigen, die für das zugrundeliegende Verfahren relevant sind.

Die Befugnis setzt entsprechend § 9 Absatz 1 voraus, dass die Maßnahme nur zur Ergänzung vorhandener Sachverhalte erfolgen kann. Voraussetzungen für ein Tätigwerden des Bundeskriminalamts ist, dass bereits Ermittlungsunterlagen vorliegen (vgl. Bundestagsdrucksache 13/1550, S. 24). Die Vorschrift setzt einen Tatverdacht bzw. zur Straftatenverhütung eine zumindest konkretisierte Gefahrenlage voraus. Schwelle ist nach Absatz 1 Satz 1 Nummer 2 eine Straftat, die auch im Einzelfall von erheblicher Bedeutung ist. Darunter fallen insbesondere – aber nicht ausschließlich – die in § 100a Absatz 2 der Strafprozessordnung enthaltenen Straftatbestände. Der Abgleich ist nach Absatz 1 Satz 1 Nummer 3 subsidiär zu anderen Maßnahmen. Der Abgleich erfolgt zielgerichtet bezogen auf einen konkreten Sachverhalt. Die erstmalige Gewinnung von Verdachts- oder Gefahrenmomenten ist nicht von der Befugnis erfasst.

Zum Zweck der Durchführung des Abgleichs nach Absatz 1 können öffentlich zugängliche Daten aus dem Internet erhoben werden. Dies erlaubt zudem die Speicherung der Daten, um diese als Referenz für den Abgleich zu verwenden. Diese temporäre Speicherung erfolgt ausschließlich zu dem Zweck des konkreten Ausgangsverfahrens, eine weitere Verwendung der Daten ist ausgeschlossen; sie sind nach Absatz 4 zu löschen.

Öffentlich zugängliche Daten können auch im Rahmen der allgemeinen Ermittlungsbefugnisse erhoben werden. Spezialgesetzlicher Regelungsbedarf besteht jedoch, da Absatz 1 Satz 1 den biometrischen Abgleich öffentlich zugänglicher Daten mittels automatisierter Verarbeitung regelt. Nur mittels einer solchen technischen Anwendung können Lichtbilder und Videos analysiert werden, die einen Abgleich ermöglicht. Ohne eine solche technische Verarbeitung könnten die erhobenen Daten nicht verwendet werden, da sich öffentlich zugängliche Daten in Format und Struktur von den im Informationssystem oder -verbund gespeicherten Daten unterscheiden.

Nach Satz 2 ist ein Abgleich mit solchen Daten unzulässig, die zum Zeitpunkt des Abgleichs ein tatsächliches Geschehen in Echtzeit widerspiegeln. Es soll damit ausgeschlossen werden, dass eine Echtzeitüberwachung bestimmter Bereiche stattfindet. Gemeint sind damit insbesondere Live-Streams, zum Beispiel von Veranstaltungen, in denen auch das Publikum erfasst wird, oder das Live-Video einer Webcam eines öffentlich zugänglichen Ortes. Erfasst sind auch Echtzeit-Lichtbild-Sequenzen, also beispielsweise die Bilder von Webcams, die in zeitlich kurzer Abfolge einzelne Lichtbilder ins Internet hochladen.

Zu Absatz 2

Absatz 2 trifft Regelungen zu den Adressaten der Befugnis nach Absatz 1. Im Rahmen der Zentralstellenaufgabe bildet die Unterstützung der Polizeien des Bundes und der Länder einen Schwerpunkt. Nummer 1 umfasst Tatverdächtige und Beschuldigte nach den zugrundeliegenden strafprozessrechtlichen Ermittlungsverfahren und im präventiven Bereich die polizeipflichtigen Personen entsprechend § 18 oder § 19 BPolG. Letzteres richtet sich im Einzelnen nach den Fachgesetzen der Polizeien des Bundes und der Länder. Zudem ist die Maßnahme gegen Anlasspersonen nach § 18 Absatz 1 Nummer 4 erlaubt.

Nach Nummer 2 darf die Maßnahme gegen Personen nach § 19 Absatz 1 Satz 1 – Zeugen, Opfer, Kontaktpersonen und Auskunftspersonen – ausschließlich zu dem Zweck der Identifizierung und Aufenthaltsermittlung sowie nach einer Abwägung mit deren schutzwürdiger Interessen erfolgen.

Zu Absatz 3

Der Abgleich nach Absatz 1 setzt voraus, dass im Informationssystem oder -verbund Daten als Grundlage des Abgleichs vorhanden sind (Beispiel: Lichtbild eines Tatverdächtigen). Absatz 3 Satz 1 stellt klar, dass § 12 Absatz 2 für die abzugleichenden Daten gilt. Die Vorgaben der hypothetischen Datenneuerhebung gelten für die gegenständliche Maßnahme. Das Bundeskriminalamt darf demnach nur solche Daten als Grundlage des Abgleichs einbeziehen, die mindestens der Verfolgung einer vergleichbar bedeutsamen Straftat dienen und aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Verfolgung solcher Straftaten ergeben. Letzteres sichert, dass nur im Einzelfall notwendige Daten zum Abgleich verwendet werden. Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen oder verdeckten Eingriff in informationstechnische Systeme erlangt wurden, können aufgrund der hohen Eingriffsintensität nicht in den Abgleich einbezogen werden.

Zu Absatz 4

Nach Absatz 4 Satz 1 dürfen ausschließlich Daten weiterverarbeitet werden, sofern sich auf Grundlage des Abgleichs ein konkreter Ermittlungsansatz aus den Daten ergibt. Die Weiterverarbeitung richtet sich im Weiteren nach den Regelungen zur Weiterverarbeitung nach diesem Gesetz oder der Strafprozessordnung. Im Übrigen sind die für die Durchführung des Abgleichs nach Absatz 1 erhobenen und verarbeiteten Daten unverzüglich zu löschen. Dies umfasst auch technische Exzerpte der erhobenen Daten, die für die technische Verarbeitung erstellt werden. Die Vorschrift sichert eine enge Zweckbindung der Daten. Satz 2 sieht vor, dass das Bundeskriminalamt die Datensicherheit mittels technisch-organisatorischer Maßnahmen gewährleisten muss. Nach Satz 3 sind die Daten nach § 82 Absatz 1 zu protokollieren; hinzu kommt nach Satz 4 die Zielperson. Dies dient der effektiven datenschutzrechtlichen Kontrolle.

Zu Absatz 5

Zur Durchführung des biometrischen Internetabgleichs nach Absatz 1 kann eine Übermittlung an andere öffentliche oder nichtöffentliche Stellen erforderlich sein, damit diese den Abgleich nach Absatz 1 Satz 1 durchführt. Absatz 5 sieht insofern eine spezielle Übermittlungsbefugnis vor. Die Vorschrift regelt die Möglichkeit, bei der Datenübermittlung an inländische Stellen sowie an Stellen eines Mitgliedsstaats der Europäischen Union von den Regelungen in § 25 Absatz 6 zur Verpflichtung Dritter zur Zweckbindung abzuweichen.

Nach Absatz 5 Nummer 1 müssen dabei die Tatbestandsvoraussetzungen nach Absatz 1 Satz 1 erfüllt sein. Absatz 5 Nummer 2 regelt die Erforderlichkeit, dass die Durchführung durch das Bundeskriminalamt selbst unmöglich oder nur bei unverhältnismäßigem Aufwand möglich ist. Dies ist der Fall, sofern technische Produkte für die Durchführung des Abgleichs nicht beschafft oder entwickelt werden können oder wenn dies nicht im Verhältnis zum zu erwartenden Erfolg des Abgleichs steht.

Zu Absatz 6

Absatz 6 entspricht im Wesentlichen Absatz 5 und trifft Regelungen für die Übermittlung an Stellen in Drittstaaten. Die Übermittlung an Stellen in Drittstaaten ist nach Absatz 6 Satz 1 Nummer 1 möglich, sofern dies zum Schutz der nationalen Sicherheit erforderlich ist.

Nach Absatz 6 Satz 1 Nummer 2 sind § 27 Absatz 8 BKAG und § 81 des Bundesdatenschutzgesetzes (BDSG) zu beachten. Unter den Voraussetzungen von § 27 Absatz 8 ist die Datenübermittlung an öffentliche und nichtöffentliche Stellen in Drittstaaten erlaubt. Hierfür gelten besondere Maßgaben nach § 81 BDSG.

Absatz 6 Satz 1 Nummer 3 entspricht Absatz 5 Nummer 2, regelt aber zusätzlich, dass auch der Abgleich durch eine inländische öffentliche oder nichtöffentliche Stelle oder eine öffentliche oder nichtöffentliche Stelle eines Mitgliedsstaats der Europäischen Union technisch unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich ist.

Nach Absatz 6 Satz 2 kann das Bundeskriminalamt, sofern es erforderlich ist, von § 81 Absatz 1 Nummer 3 und Absatz 4 BDSG abweichen. § 27 Absatz 8 in Verbindung mit § 81 des Bundesdatenschutzgesetzes setzt Artikel 39 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates um. Die Richtlinie (EU) 2016/680 regelt jedoch nicht die Verarbeitung personenbezogener Daten bei Tätigkeiten, die nicht unter das Unionsrecht fallen. Dies betrifft die nationale Sicherheit betreffende Tätigkeiten sowie Tätigkeiten von Agenturen oder Stellen, die mit Fragen der nationalen Sicherheit befasst sind (Erwägungsgrund 14) und spiegelt den in Artikel 4 Absatz 2 Satz 3 des Vertrags über die Europäische Union primärrechtlich verankerten Vorbehalt der alleinigen Verantwortung der einzelnen Mitgliedsstaaten für die nationale Sicherheit wider.

Unter den Begriff der nationalen Sicherheit nach Artikel 4 Absatz 2 Satz 3 des Vertrags über die Europäische Union fällt nach der Rechtsprechung des Europäischen Gerichtshofs das zentrale Anliegen „die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft zu schützen, und umfasst die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie insbesondere terroristische Aktivitäten.“ (Europäischer Gerichtshof, Urteil vom 6. Oktober 2020, Rechtssachen C-511/18, C-512/18 und C-520/18, Randnummer 135).

Darunter fallen Tätigkeiten des Bundeskriminalamts im Bereich der Abwehr, Verhütung und Verfolgung von Terrorismus, Spionage, Sabotage und Straftaten einer § 5 Absatz 1 Satz 2 vergleichbaren Dimension. Das Bundesverfassungsgericht (BVerfG) führt zu der Vorgängerauslegung von § 5 Absatz 1 Satz 2 aus: „Straftaten mit dem Gepräge des Terrorismus in diesem Sinne zielen auf eine Destabilisierung des Gemeinwesens und umfassen hierbei in rücksichtsloser Instrumentalisierung anderer Menschen Angriffe auf Leib und Leben beliebiger Dritter. Sie richten sich gegen die Grundpfeiler der verfassungsrechtlichen Ordnung und das Gemeinwesen als Ganzes.“ (BVerfG, Urteil vom 24. April 2016, Az. 1 BvR 966/09 u.a., Randnummer 96).

Zu Absatz 7

Die Absätze 5 und 6 sind spezialgesetzliche Übermittlungsregelungen für den Zweck der Befugnis. Absatz 7 stellt klar, dass die Regelungen zur Datenübermittlung in §§ 25 bis 28 im Übrigen Anwendung finden.

Zu Absatz 8

Nach Absatz 8 Satz 1 besteht die Notwendigkeit eines richterlichen Beschlusses nach entsprechendem Antrag der Amtsleitung des Bundeskriminalamts für die Anordnung der Maßnahme nach Absatz 6, das bedeutet die Übermittlung von Daten an eine öffentliche oder nichtöffentliche Stelle in einem Drittstaat und die Durchführung des biometrischen Abgleichs nach Absatz 1 durch diese Stelle. Sätze 2 und 3 enthalten eine Regelung zur Anordnung bei Gefahr im Verzug. Nach Satz 4 kann eine Delegation der Antragsbefugnis sowie der Anordnungsbefugnis bei Gefahr im Verzug auf Bedienstete des

Bundeskriminalamts mit Befähigung zum Richteramt übertragen werden. Die Übertragung kann im Einzelfall oder im Wege einer allgemeinen Weisung erfolgen.

Zu § 9b

Das Bundesverfassungsgericht hat in seinem Urteil vom 16. Februar 2023 zur automatisierten Datenanalyse (Az. 1 BvR 1547/19, 1 BvR 2634/20) die verfassungsrechtliche Legitimität von Befugnissen zur automatisierten Datenanalyse bestätigt und die verfassungsrechtlichen Anforderungen an entsprechende Vorschriften konkretisiert. Die neuen Regelungen in §§ 9b und 63c setzen diese Anforderungen um.

Die Einrichtung und Nutzung einer automatisierten Anwendung zur Datenanalyse ist für die Aufgabenerfüllung des Bundeskriminalamts erforderlich. Ausgangspunkt ist das stetige Ansteigen der vorhandenen Daten, welche durch das Bundeskriminalamt ausgewertet werden müssen. Es bedarf insofern einer Fortentwicklung der technischen Instrumente zur Bewältigung der polizeilichen Aufgaben. Ein Baustein dafür sind Anwendungen zur automatisierten Datenanalyse. Im Vergleich zum Datenabgleich zeichnen sich automatisierte Datenanalysen dadurch aus, dass sie darauf gerichtet sind, neues Wissen zu erzeugen (BVerfG, a. a. O., Randnummer 67).

Das Bundesverfassungsgericht hat in seinem Urteil vom 16. Februar 2023 Kriterien dafür aufgestellt, unter welchen Umständen Eingriffe durch Datenverarbeitungen eine besondere Eingriffsintensität erreichen, die einer spezifischen gesetzlich zu regelnden Eingriffsschwelle bedürfen. Dazu gehören unter anderem die Fähigkeit der Auswertung großer und komplexer Informationsbestände (BVerfG, a. a. O., Randnummer 69) als auch der Einsatz komplexer Formen des Datenabgleichs (BVerfG, a. a. O., Randnummer 90), wobei es sich jeweils nur um Anhaltspunkte zur Bestimmung der Eingriffsintensität handelt.

Die hier eingeführten Vorschriften ermöglichen es dem Bundeskriminalamt, unter Wahrung der verfassungsrechtlichen Voraussetzungen entsprechende Datenanalysen vorzunehmen. Dabei sollen die Datenbestände, die beim Bundeskriminalamt bereits aufgrund bestehender Rechtsgrundlagen rechtmäßig erlangt und gespeichert werden, ausschließlich zum Zwecke der Analyse zusammengeführt und weiterverarbeitet werden. Das Bundeskriminalamt wird auf diese Weise in die Lage versetzt, bereits bei ihm im polizeilichen Informationssystem oder im polizeilichen Informationsverbund nach § 29 vorhandene Informationen besser, schneller und effizienter auszuwerten. Die Befugnisse zur Weiterverarbeitung von personenbezogenen Daten nach § 16 Absatz 1 und für den (ebenfalls automatisierten) Datenabgleich nach § 16 Absatz 4 bleiben von dieser Regelung unberührt.

Eine entsprechende Befugnis ist neben der hier betroffenen Zentralstellenregelung zur Abwehr von Gefahren des internationalen Terrorismus (§ 39b) und zum Schutz von Mitgliedern der Verfassungsorgane und der Leitung des Bundeskriminalamts (§ 63c) vorgesehen.

Zu Absatz 1

Absatz 1 regelt die Befugnis des Bundeskriminalamts, die Daten, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, mittels einer automatisierten Anwendung zur Datenanalyse aus verschiedenen Datenbeständen technisch zusammenzuführen. Er regelt ferner die Befugnis, diese zusammengeführten Daten zu analysieren, wenn dies zur Erfüllung der Zentralstellenaufgabe des Bundeskriminalamts erforderlich ist. Die besondere verfassungsrechtliche Rolle des Bundeskriminalamts als Zentralstelle für das polizeiliche Auskunftswesen und Nachrichtenwesen und für die Kriminalpolizei erfordert hohe Fähigkeiten im Bereich der Auswertung und Analyse von Daten. Als Zentralstelle hat das Bundeskriminalamt insbesondere den gesetzlichen Auftrag, Informationen zu sammeln und auszuwerten und muss daher auch mit den rechtlichen sowie technischen Mitteln ausgestattet werden, die es in die Lage versetzen, diesen Auftrag bestmöglich zu erfüllen. Gemäß § 2 Absatz 1 steht dabei die Unterstützung der Polizeien des Bundes oder Länder, die in der Regel die

zugrundeliegenden Verfahren führen, im Vordergrund. Zweck der Befugnis ist die Erstellung einer Analyse für die Zwecke des zugrundeliegenden Verfahrens. Dies umfasst Verfahren zur Gefahrenabwehr, Straftatenverhütung und Strafverfolgung.

Voraussetzung ist zunächst, dass dies im Rahmen der Befugnisse des Bundeskriminalamts als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei zur Verfolgung oder Verhütung einer Straftat erforderlich ist. Der Einsatz entsprechender Analysen unterliegt einer angemessenen Eingriffsschwelle. Nach dem Urteil des Bundesverfassungsgerichts vom 16. Februar 2023 kann die automatisierte Datenanalyse bei einer hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgütern erfolgen (BVerfG, a. a. O., Randnummer 105f.). Der Tatbestand entspricht der Rechtsprechung des Bundesverfassungsgerichts zu den Anforderungen an eine konkretisierte Gefahrenlage (Urteil vom 20. April 2016, Az. 1 BvR 966/09 und 1 BvR 1140/09, Randnummer 165). Die präventive Regelung in § 9b Absatz 1 Nummer 2 sieht vor, dass eine konkretisierte Gefahrenlage für die Begehung einer Straftat nach § 100a Absatz 2 der Strafprozessordnung bestehen muss und kumulativ die vom Bundesverfassungsgericht anerkannten besonders gewichtigen Rechtsgüter gefährdet sind (BVerfG, a. a. O., Randnummer 105f.).

Die repressive Aufgabenwahrnehmung des Bundeskriminalamts in seiner Zentralstellenfunktion ist in § 9b Absatz 1 Nummer 1 geregelt. Das Bundesverfassungsgericht sieht als maßgebliches Kriterium für die Rechtfertigung von repressiven Befugnissen das Gewicht der verfolgten Straftaten an (Urteil vom 20. April 2016, Az. 1 BvR 966/09 und 1 BvR 1140/09, Randnummer 106). Eingriffsintensive Überwachungsmaßnahmen – beispielsweise – Telekommunikationsüberwachung erfordern demnach den Verdacht einer schweren Straftat, während besonders eingriffsintensive Überwachungsmaßnahmen – Wohnraumüberwachung und Zugriff auf informationstechnische Systeme – den Verdacht einer besonders schweren Straftat erfordern (Urteil vom 20. April 2016, Az. 1 BvR 966/09 und 1 BvR 1140/09, Randnummer 107). Das Bundesverfassungsgericht hat präventive Befugnisse zur automatisierten Datenanalyse – in der gegenständlichen Ausgestaltung – als eingriffsintensive heimliche Überwachungsmaßnahme eingestuft (Urteil vom 16. Februar 2023, Az. 1 BvR 1547/19, 1 BvR 2634/20, Randnummer 105). Für die Rechtfertigung ist somit der Straftatenkatalog des § 100a Absatz 2 der Strafprozessordnung, der schwere Straftaten umfasst, angemessen. Überdies ist erforderlich, dass die verfolgte Straftat auch im Einzelfall schwer wiegt (zur Speicherung von Telekommunikationsdaten: BVerfG, Az. 1 BvR 256/08, Randnummer 229).

Die automatisierte Datenanalyse bezieht sich nur auf Daten, auf die es zur Erfüllung seiner Aufgaben zugreifen darf. Die Formulierung entspricht dem Datenabgleich nach § 16 Absatz 4. Daraus ergibt sich weder die Befugnis zur Erhebung der abzugleichenden Daten noch zur Speicherung dieser Daten. Das Bundeskriminalamt kann demnach nur Daten in die automatisierte Datenanalyse einbeziehen, die ihm schon bekannt sind (Bundestagsdrucksache 13/1550, Seite 36). Dazu zählen beim Bundeskriminalamt gespeicherte Daten aus den polizeilichen Auskunftssystemen einschließlich der Daten aus dem polizeilichen Informationsverbund, Vorgangs- und Falldaten (insbesondere aus laufenden Ermittlungs- und Gefahrenabwehrvorgängen) und Daten aus Asservaten. Dies umfasst auch Telekommunikations-, Verkehrs- und Nutzungsdaten.

Die Daten können nur dann schnell und effizient analysiert werden, wenn zumindest der Grunddatenbestand bereits zusammengeführt und aktualisiert in einem einheitlichen Datenformat in einer entsprechenden Anwendung vorliegt. Der Vorgang der Zusammenführung und Formatierung ist aufgrund der Masse der Daten aufwändig, so dass eine Zusammenführung lediglich im Einzelfall dem gewünschten Zweck der schnellen und effektiven Straftatenverhütung und -verfolgung nicht gerecht werden könnte. Die technische Zusammenführung der Daten sichert die Verarbeitbarkeit der Daten im Rahmen der automatisierten Datenanalyse. Die Zusammenführung muss daher aus technischen Gründen vom Einzelfall und weiteren Eingriffsschwellen unabhängig sein. Die konkrete Ausgestaltung hängt von der technischen Lösung ab. Die Zusammenführung dient ausschließlich dem Zweck

der automatisierten Datenanalyse im konkreten Einzelfall. Die Vorgaben des Bundeskriminalamtgesetzes zur Weiterverarbeitung der Daten bleiben davon unberührt. Dies umfasst insbesondere die Einhaltung der Vorgaben zur hypothetischen Datenneuerhebung nach § 12, zur Kennzeichnung nach § 14, zur Regelung von Zugriffsberechtigungen nach § 15 und zu den Aussonderungsprüffristen nach § 77.

Zu Absatz 2

Absatz 2 Satz 1 trifft Regelungen zu den Adressaten der Befugnis nach Absatz 1. Es wird auf die Begründung zu § 9a Absatz 2 verwiesen.

Zu Absatz 3

Die Befugnis berechtigt das Bundeskriminalamt, die automatisierte Analyse interner Datenbestände durchzuführen. Nach Absatz 3 Satz 1 ist es ausgeschlossen, dass eine direkte Anbindung der Anwendung zur automatisierten Datenanalyse an Register, die nicht in den Anwendungsbereich der Richtlinie (EU) 2016/680 fallen, und an Internetdienste erfolgt. Demnach ist es nicht von der Befugnis umfasst, die automatisierte Datenanalyse unmittelbar in externen/öffentlichen Datenquellen wie zum Beispiel aus Internetdiensten wie Social-Media Plattformen durchzuführen. Daten aus externen Quellen können jedoch im konkreten Einzelfall nach Absatz 3 Satz 2 in die Analyse miteinbezogen werden, wenn diese bereits im Vorfeld auf Basis einer entsprechenden Befugnisnorm zur Datenerhebung rechtmäßig erhoben wurden und weiterhin rechtmäßig gespeichert in dem Informationssystem des Bundeskriminalamts vorliegen oder zwischengespeichert werden, ohne dass es zu einer längerfristigen Speicherung der Daten kommt.

Zu Absatz 4

Absatz 4 Nummer 1 bis 5 enthält eine abschließende Aufzählung der möglichen Formen der Weiterverarbeitung im Rahmen einer automatisierten Anwendung zur Datenanalyse.

Zu Absatz 5

Absatz 5 Satz 1 stellt eine gesetzliche Sicherung vor den spezifischen Risiken diskriminierender Algorithmen dar und verpflichtet das Bundeskriminalamt zu technisch-organisatorischen Maßnahmen bei der Verwendung dieser Systeme.

Satz 2 verweist auf die besonderen Datenverarbeitungsregelungen des Bundeskriminalamtgesetzes. Nach Absatz 1 bezieht sich die automatisierte Datenanalyse auf alle Daten, auf die das Bundeskriminalamt zur Erfüllung seiner Aufgaben zugreifen darf. Satz 2 stellt klar, dass dabei die Anforderungen der hypothetischen Datenneuerhebung nach § 12 gelten. Die Vorschrift verweist zudem auf die besondere Zweckbindung von Daten, die nach § 22 Absatz 2 weiterverarbeitet werden gelten. Ebenso unberührt bleiben Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung: Die Verwendungs- und Verwertungsverbote der Datenerhebungsbefugnisse nach Bundeskriminalamtgesetz und Strafprozessordnung für Inhalte, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, sind bei der automatisierten Datenanalyse zu beachten.

Satz 3 regelt besondere Verbote für die Weiterverarbeitung nach Satz 1. Die Regelungen in Satz 3 stellt klar, dass die polizeiliche Aufgabenerfüllung Bediensteten des Bundeskriminalamts verantwortet wird. Die automatisierte Datenanalyse nimmt dafür eine unterstützende Funktion ein. Die Anordnung von Anschlussmaßnahmen gegen bestimmte Personen unterliegt keiner Automatisierung. Nach Satz 3 ist daher eine im Sinne von Artikel 11 Absatz 1 der Richtlinie (EU) 2016/680 automatisierte Einzelfallentscheidung, die alleine aufgrund der automatisierten Datenanalyse erfolgt, verboten.

Zu Absatz 6

IT-Produkte, die zur Durchführung der automatisierten Datenanalyse verwendet werden, dürfen nach Absatz 6 Satz 1 nur von entsprechend geschultem Personal bedient werden. Nur geschultem Personal darf nach § 15 die Zugriffsberechtigung erteilt werden. Satz 2 sieht vor, dass das Bundeskriminalamt die Datensicherheit mittels technisch-organisatorischer Maßnahmen gewährleisten muss. Nach Satz 3 sind die Daten nach § 82 Absatz 1 zu protokollieren; hinzu kommt nach Satz 4 die Zielperson. Dies dient der effektiven datenschutzrechtlichen Kontrolle. Nach Satz 5 ist die Übermittlung an andere Stellen zur Durchführung der automatisierten Datenanalyse nach Absatz 1 ausgeschlossen.

Für IT-Produkte, die das Bundeskriminalamt für die Durchführung der automatisierten Datenanalyse verwendet, gelten im Übrigen die allgemeinen datenschutzrechtlichen Anforderungen. Die oder der Datenschutzbeauftragte des Bundeskriminalamts nach § 70 BKAG ist gemäß § 7 Absatz 1 Satz 1 Nummer 2 BDSG für die Überwachung der Einhaltung der datenschutzrechtlichen Vorgaben durch das Bundeskriminalamt zuständig. Für Produkte, die für die automatisierte Datenanalyse eingesetzt werden, bedarf es einer Datenschutz-Folgenabschätzung nach § 67 BDSG, bei der die oder der Datenschutzbeauftragte des Bundeskriminalamts nach § 7 Absatz 1 Satz 1 Nummer 3 und § 67 Absatz 3 BDSG zu beteiligen ist. Zudem sind die Verarbeitungen durch die automatisierte Datenanalyse im Verzeichnis von Verarbeitungstätigkeiten nach § 80 BKAG in Verbindung mit § 70 BDSG zu ergänzen.

Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat nach § 14 Absatz 1 Satz 1 Nummer 1 BDSG die Aufgabe, die Einhaltung der datenschutzrechtlichen Vorgaben zu überwachen und durchzusetzen. Vor der Inbetriebnahme von IT-Produkten zur automatisierten Datenanalyse ist eine Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach § 69 BDSG erforderlich. Zu den datenschutzrechtlichen Befugnissen der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gehören unter anderem die Beanstandung nach § 16 Absatz 2 Satz 1 BDSG und die Anordnung geeigneter Maßnahmen zur Beseitigung eines erheblichen Verstoßes gegen datenschutzrechtliche Vorschriften nach § 69 Absatz 2 BKAG.

Soweit der bezüglich der verwendeten IT-Produkte der Anwendungsbereich der Verordnung (EU) 2024/1689 (KI-Verordnung) eröffnet ist, gelten die entsprechenden Vorgaben unmittelbar und sind bereits beim Design und Training zu berücksichtigen. Ein zentraler Baustein ist das Risikomanagementsystem nach Artikel 9 der Verordnung (EU) 2024/1689, das vor Inverkehrbringen und während des gesamten Lebenszyklus des KI-Systems sicherstellen soll, dass etwaige Risiken für Grundrechte, Gesundheit oder Sicherheit – einschließlich solcher durch diskriminierende Ergebnisse – frühzeitig erkannt, minimiert und überwacht werden. Artikel 9 Absatz 2 Buchstabe c verpflichtet insbesondere zur fortlaufenden Überwachung der KI-Leistung und zum Umgang mit Abweichungen und Fehlverhalten. Darüber hinaus schreibt Artikel 10 Absatz 2 Buchstabe f der Verordnung (EU) 2024/1689 vor, dass bei den für Training, Validierung und Tests verwendeten Datensätzen eine sorgfältige Prüfung auf mögliche Verzerrungen („Bias“) erfolgen muss, die sich negativ auf Grundrechte oder gesetzlich geschützte Merkmale auswirken könnten. Nach Artikel 10 Absatz 3 Satz 1 der Verordnung (EU) 2024/1689 müssen die Datensätze ferner „relevant, hinreichend repräsentativ, fehlerfrei und vollständig“ sein – dies ist besonders wichtig zur Vermeidung strukturell benachteiligender Trainingsgrundlagen. Ergänzend verlangt Artikel 13 der Verordnung (EU) 2024/1689 Maßnahmen zur Transparenz: Hochrisiko-KI-Systeme müssen so gestaltet sein, dass ihre Ausgaben für den Nutzer verständlich sind und dieser die Ergebnisse sachgerecht bewerten kann. Auch dies dient mittelbar der Kontrolle und Korrektur diskriminierender Tendenzen. Nach Artikel 14 der Verordnung (EU) 2024/1689 muss zudem eine menschliche Aufsicht gewährleistet werden, um beispielsweise potenziell diskriminierende Entscheidungen erkennen und korrigieren zu können. Die Aufsichtspersonen müssen angemessen geschult und befugt sein (Artikel 14 Absatz 4).

Zu Absatz 7

Nach Absatz 7 besteht eine besondere Anordnungsbefugnis für die Maßnahme nach Absatz 1. Die Anordnung obliegt der Präsidentin oder dem Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung oder Bediensteten des Bundeskriminalamts mit Befähigung zum Richteramt.

Zu Nummer 3 (§ 22)

Zu Buchstabe a

Die Änderung der Überschrift von § 22 folgt aus der Einfügung der Absätze 3 und 4. Die Aufzählung der einzelnen Verarbeitungszwecke wird gestrichen.

Zu Buchstabe b

Die Befugnis zum Testen von IT-Produkten sowie Trainieren von selbstlernenden Systemen ist für die Nutzung von IT-Anwendungen des Bundeskriminalamts von entscheidender Bedeutung. Für die (Weiter-)Entwicklung solcher Anwendungen können mehrstufige Testzyklen erforderlich sein, die unter Umständen auch die Verwendung von pseudonymisierten oder Echtdaten erfordern. Dies gilt für eigene IT-Anwendungen des Bundeskriminalamts als auch im Einzelfall für die Unterstützung im Rahmen der Aufgabe des Bundeskriminalamts als Zentralstelle.

Zu Absatz 3

Der neue § 22 Absatz 3 Satz 1 schafft eine ausdrückliche Rechtsgrundlage für die Entwicklung, Überprüfung, Änderung und das Trainieren von IT-Produkten durch das Bundeskriminalamt anhand von Echtdaten. IT-Produkte sind entsprechend der Legaldefinition in § 2 Absatz 9a des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten. Ausdrücklich genannt ist das Training selbstlernender Systeme.

Auch wenn das Testen von IT-Produkten mittels personenbezogener Daten in der Regel eine technisch-organisatorische Maßnahme zur Gewährleistung der Sicherheit der Datenverarbeitung im Produktivbetrieb darstellt, die auf Artikel 6 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119/1 vom 4. Mai 2016, S. 1), im Folgenden Datenschutz-Grundverordnung, in Verbindung mit Artikel 32 der Datenschutz-Grundverordnung beziehungsweise § 64 des Bundesdatenschutzgesetzes gestützt werden kann, soll aus Gründen der Rechtssicherheit eine spezialgesetzliche Rechtsgrundlage geschaffen werden.

Erfüllt das Testen und Trainieren von IT-Produkten im Einzelfall die für die wissenschaftliche Forschung kennzeichnenden Merkmale, ist § 21 als Rechtsgrundlage für die Datenverarbeitung für die wissenschaftliche Forschung heranzuziehen.

Eine Verarbeitung personenbezogener Daten durch das Bundeskriminalamt nach § 22 Absatz 3 Satz 1 ist ausschließlich zum Zwecke der Entwicklung, Überprüfung, Änderung und des Trainierens von IT-Produkten zulässig. Zudem muss es sich um IT-Produkte handeln, die das Bundeskriminalamt für die eigene Aufgabenwahrnehmung entwickelt oder nutzt. Die Datenverarbeitung muss zur Erreichung der benannten Zwecke erforderlich sein. Insbesondere muss ein Bedürfnis für unveränderte Daten bestehen oder eine Anonymisierung oder Pseudonymisierung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich sein. Die Aufzählung der Gründe für die Erforderlichkeit der Datenverarbeitung ist nicht abschließend.

Satz 2 dient dem besonderen Schutz von Daten, die aus den in § 12 Absatz 3 genannten besonders eingriffsintensiven Maßnahmen stammen. IT-Produkte, einschließlich selbstlernender Systeme, dürfen nicht mit Daten, die aus besonders eingriffsintensiven Maßnahmen stammen, trainiert werden. Dies dient dem Schutz der besonders eingriffsintensiv erhobenen Daten. Für die Entwicklung, Überprüfung und Änderung dieser Daten durch das Bundeskriminalamt gilt dieses Verbot nicht. IT-Produkte des Bundeskriminalamts sind vor größeren technischen Umstellungen in einer separaten Schutzumgebung zu testen. Unter solchen technischen Umstellungen sind zum Beispiel der Umzug der Betriebsumgebung, der Rollout eines neuen Produkts oder ein umfangreiches Update zu verstehen. Ziel der Testung in einer separaten Schutzumgebung ist die Feststellung von Schwachstellen und die Sicherung der Funktionsfähigkeit im Betrieb. Personenbezogene Daten nach § 12 Absatz 3 können notwendiger Teil dieser Betrachtung in der Testumgebung sein und müssen in diesen Fällen einbezogen werden. Insbesondere sind technisch-organisatorische Vorkehrungen nach § 12 Absatz 5 zu treffen, die der Sicherstellung der Vorgaben der hypothetischen Datenneuerhebung dienen. Die Vorkehrungen müssen zwingend Bestandteil des Teststadiums sein.

Satz 3 regelt den technisch-organisatorischen Schutz der Datensicherheit durch das Bundeskriminalamt. Dies entspricht der Regelung in § 21 Absatz 6 zur Weiterverarbeitung von personenbezogenen Daten für die wissenschaftliche Forschung.

Zu Absatz 4

Absatz 4 Satz 1 ist eine spezialgesetzliche Übermittlungsvorschrift zum Testen und Trainieren an öffentliche oder nichtöffentliche Stellen in Deutschland, in einem Mitgliedsstaat der Europäischen Union oder einem Drittstaat. Es müssen kumulativ die Voraussetzungen von Absatz 3 sowie die spezifische Erforderlichkeit der Übermittlung an eine andere Stelle vorliegen. Satz 2 stellt klar, dass für die Übermittlung § 28 gilt.

Satz 3 schließt die Übermittlung von Daten, die aus den in § 12 Absatz 3 genannten besonders eingriffsintensiven Maßnahmen stammen, aus.

Die Regelungen in den Sätzen 4 und 5 stellen sicher, dass Dritte zum Beispiel im Rahmen einer Auftragsverarbeitung nur tätig werden dürfen, wenn sichergestellt ist, dass die Verarbeitung personenbezogener Daten nur durch Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete oder zur Geheimhaltung verpflichtete Mitarbeiterinnen oder Mitarbeiter erfolgt. Dies entspricht der Regelung in § 21 Absatz 4 zur Weiterverarbeitung von personenbezogenen Daten für die wissenschaftliche Forschung.

Satz 6 regelt die besondere Zweckbindung bezüglich der Weiterverarbeitung der übermittelten Daten durch einen Dritten. Nach Satz 7 weist das Bundeskriminalamt die Stelle auf diese Zweckbindung hin.

Nach Satz 8 gelten die Vorgaben zur Datensicherheit entsprechend Absatz 3 Satz 3.

Soweit der Anwendungsbereich der Verordnung (EU) 2024/1689 eröffnet ist, gelten die Ausführungen zu § 9b Absatz 6.

Zu Nummer 4

Zu § 63b

§ 63b regelt die Befugnis zum biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet zum Zweck des Schutzes von Mitgliedern der Verfassungsorgane und der Leitung des Bundeskriminalamts. Insbesondere die Radikalisierung in der sogenannten Reichsbürger- und Querdenkerszene und die damit verbundene erhöhte Gefährdungslage für die Repräsentanten des Rechtsstaats und der Verfassungsorgane erfordern auch für

diesen Aufgabenbereich adäquate rechtliche Befugnisse und technische Fähigkeiten. Aber auch in anderen Phänomenbereichen sind gleichgelagerte Gefahren denkbar. Es wird auf die Begründung zu § 9a verwiesen.

Die in Absatz 1 Nummer 3 geregelte Tatbestandsvariante bezieht sich auf das individuelle Verhalten einer Person und erfordert nicht, dass Tatsachen ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennen lassen. Das Bundesverfassungsgericht hat eine solche Tatbestandsvariante im Bereich des Terrorismus anerkannt (Urteil vom 20. April 2016, Az. 1 BvR 966/09 und 1 BvR 1140/09, Randnummer 112). Das Bundesverfassungsgericht begründete dies damit, dass terroristische Straftaten oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden (ebenda). Die Aufgabe nach § 6 unterscheidet sich von der Aufgabe der Abwehr des Terrorismus insofern, als dass nicht der Schutz der Allgemeinheit im Vordergrund steht, sondern der Schutz von Mitgliedern der Verfassungsorgane und der Leitung des Bundeskriminalamts zu schützenden Personen. Inhaltlich weisen beide Aufgaben jedoch eine vergleichbare Ausgangslage auf, insbesondere besteht eine inhaltliche Schnittmenge zwischen Terrorismus und einem Angriff auf nach § 6 geschützte Personen. Unabhängig von der Zielrichtung können solche Angriffe zudem eine Bedrohungs- und Destabilisierungswirkung erzielen, die terroristischen Angriffen vergleichbar ist. Bei der Abwehr möglicher Angriffe auf nach § 6 geschützte Personen bedarf es daher ebenfalls der Möglichkeit, Maßnahmen gegen Personen aufgrund ihres individuellen Verhaltens einzuleiten, sofern eine konkrete Wahrscheinlichkeit für die Begehung einer Straftat in einem übersehbaren Zeitraum besteht.

Zu § 63c

§ 63c regelt die Befugnis zur automatisierten Datenanalyse zum Zweck des Schutzes von Mitgliedern der Verfassungsorgane und der Leitung des Bundeskriminalamts. Es wird auf den in der Begründung zu § 63b ersichtlichen Bedarf verwiesen.

Der Tatbestand von § 63c Absatz 1 Satz 1 richtet sich auf die Abwehr von Gefahren für Leib, Leben oder Freiheit der geschützten Personen. § 63c Absatz 1 Satz 2 entspricht der Rechtsprechung des Bundesverfassungsgerichts zu den Anforderungen an eine konkretisierte Gefahrenlage für besonders gewichtige Rechtsgüter (Urteil vom 20. April 2016, Az. 1 BvR 966/09 und 1 BvR 1140/09, Randnummer 105f., 165). Bezüglich der tatbestandlichen Schwelle in Satz 2 Nummer 2 wird auf die Begründung zu § 63b verwiesen. Im Übrigen wird auf die Begründung zu § 9b verwiesen.

Zu Artikel 2 (Änderung des Bundespolizeigesetzes)

Zu Nummer 1

Zu Buchstabe a

Es handelt sich um eine redaktionelle Änderung des Inhaltsverzeichnisses aufgrund der Änderung des Überschrift von § 46.

Zu Buchstabe b

Es handelt sich um eine redaktionelle Änderung des Inhaltsverzeichnisses aufgrund der Einfügung der §§ 58a und 58b.

Zu Nummer 2

Zu Buchstabe a

Zu Buchstabe b

Der neue § 46 Absatz 3 und 4 schafft eine ausdrückliche Rechtsgrundlage für die Entwicklung, Überprüfung, Änderung und das Trainieren von IT-Produkten durch die Bundespolizei anhand von Echtdateien. Auf die Begründung zu § 22 Absatz 3 und 4 BKAG wird verwiesen.

Zu Nummer 3

Zu § 58a

§ 58a regelt die Befugnis der Bundespolizei, zur Erfüllung einer ihr obliegenden Aufgabe Daten, auf die sie zur Erfüllung ihrer Aufgaben zugreifen darf, mit öffentlich zugänglichen personenbezogenen Daten aus dem Internet mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abzugleichen.

Die Eingriffsschwellen und Schutzgüter folgen aus dem spezifischen bundespolizeilichen Aufgabenbereich. Gemäß § 2 Absatz 2 Nummer 2 Buchstabe c BPolG ist die Bundespolizei im Rahmen des Grenzschutzes zuständig für die Abwehr von Gefahren. Unerlaubte Grenzübertritte werden vorrangig in Form von Schleusungen organisiert (§§ 96f. des Aufenthaltsgesetzes). Von Schleusungen kann eine erhebliche Gefahr für Leib, Leben oder Freiheit der Geschleusten ausgehen. Insbesondere im Falle von Behältnisschleusungen (etwa bei hohen Temperaturen oder bei fehlender ausreichender Sauerstoffversorgung) ist per se von einer Gefährdung von Leib und Leben der Geschleusten auszugehen. Ferner werden alle Formen der Schleusung regelmäßig in Form von organisierter Kriminalität und damit banden- und gewerbsmäßig durchgeführt. Gemäß § 3 BPolG ist die Bundespolizei ferner zuständig für die Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung, die auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes, die den Benutzern, den Anlagen oder dem Betrieb der Bahn drohen, beim Betrieb der Bahn entstehen oder von den Bahnanlagen ausgehen. Die Zuständigkeit der Bundespolizei für die Sicherheit des Luftverkehrs ergibt sich aus § 4 BPolG, jene für die Sicherheit des Seeverkehrs aus § 7 BPolG. Auch Eingriffe in die Sicherheit der Anlagen oder des Betriebs des Luft-, See- oder Bahnverkehrs können erhebliche, auch lebensgefährdende Auswirkungen auf eine Vielzahl von Personen haben. Gemäß § 6 BPolG ist die Bundespolizei ferner zuständig für den Schutz von Verfassungsorganen des Bundes und von Bundesministerien. Angriffe auf Bundesorgane können Auswirkungen auf die Aufrechterhaltung der Staats- und Regierungsfähigkeit haben.

Ziel der Maßnahme kann es unter anderem sein, Hinweise auf den Aufenthaltsort von Schleusern und Saboteuren zu erhalten. Diese sind im Rahmen der Fahndung nach solchen Personen von wesentlicher Bedeutung, um eine Schadensverwirklichung oder -vertiefung durch die Festnahme der Personen zu verhindern. Ebenso können Verbindungen zwischen Personen und Strukturen durch biometrische Übereinstimmungen ermittelt werden. Zudem können im Rahmen der Gefahrenabwehr beispielsweise Schleuser auf Grundlage von Handyvideos der Geschleusten mittels des biometrischen Abgleichs mit öffentlich zugänglichen Daten aus dem Internet identifiziert und im weiteren Verlauf festgenommen werden. Dies ist insbesondere bei gerade andauernden Behältnisschleusungen relevant, bei denen polizeiliches Handeln zur Abwehr von Gefahren für Leib und Leben dringend geboten ist.

Im Übrigen wird auf die Begründung zu § 9a BKAG verwiesen.

Zu § 58b

Die Bundespolizei muss zur Erfüllung ihrer Aufgaben eine wachsende Anzahl von Daten auswerten und miteinander verknüpfen. Dies kann sinnvoll nur über technische Anwendungen geschehen. Der Gesetzentwurf trägt den technischen Möglichkeiten und den Bedarfen der Zeit Rechnung, indem er die Voraussetzung für die Nutzung von Softwares zur automatisierten Datenanalyse durch die Bundespolizei schafft. Bei der konkreten Ausgestaltung insbesondere auch der Eingriffsschwellen wurde den Anforderungen des Bundesverfassungsgerichts im Urteil vom 16. Februar 2023, Az. 1 BvR 1547/19 u. a. Rechnung getragen. Auf die Begründung zu § 9b des Bundeskriminalamtsgesetzes wird verwiesen.

Die Schutzgüter folgen aus dem spezifischen bundespolizeilichen Aufgabenbereich. Auf die Begründung zu § 58a BPolG wird verwiesen. Im Bereich der häufig lebensgefährlichen Schleusungen ist das Erkennen von Tat- und Täterzusammenhängen von entscheidender Bedeutung, um die häufig organisiert agierenden Täterstrukturen zu zerschlagen.

Der Luft-, See- und Bahnverkehr ist als wichtige Infrastruktur zunehmend hybriden Bedrohungen und Sabotageakten ausgesetzt. Das Risiko ist angesichts der weltpolitischen Lage als steigend einzuschätzen. Die einzelnen Sabotageakte lassen sich ohne die Möglichkeit der automatisierten Datenanalyse häufig nicht bestimmten Tätergruppierungen zuordnen und können fälschlicherweise als unzusammenhängende Einzelfälle scheinen. Auch hier ist das Erkennen von Täter- und Tatzusammenhängen für die Abwehr von Gefahren zentral.

Auch Angriffe auf Bundesorgane (§ 6 BPolG) können durch organisierte Tätergruppierungen durchgeführt werden. Hier ist es ebenfalls zentral für das Erkennen von Täter- und Tatzusammenhängen, vorhandene Daten strukturiert zusammenführen zu können.

Zu Nummer 4

Zu Buchstabe a

Die neu geschaffenen §§ 58a und 58b werden durch die Änderung der Protokollierungspflicht nach § 85 Absatz 1 unterworfen.

Zu Buchstabe b

Zu Doppelbuchstabe aa

Es handelt sich um eine redaktionelle Folgeänderung der Einfügung von § 85 Absatz 2 Nummer 8.

Zu Doppelbuchstabe bb

§ 85 Absatz 2 Nummer 8 sieht vor, dass neben den nach § 85 Absatz 1 erforderlichen Angaben bei den Maßnahmen nach §§ 58 und 58b ferner die Zielperson zu protokollieren ist.

Zu Artikel 3 (Änderung des Asylgesetzes)

Zu Nummer 1

Das Bundesamt für Migration und Flüchtlinge (BAMF) hat nach § 16 Absatz 1 Satz 1 Asylgesetz (AsylG) die Aufgabe die Identität eines Ausländers, der um Asyl nachsucht, durch erkennungsdienstliche Maßnahmen zu sichern. Angesichts der großen Bedeutung der verlässlichen und gesicherten Identitätsklärung für die Durchführung des Asylverfahrens ist es für das BAMF notwendig, die Befugnis zum biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet zu erhalten. Nach der Regelung des § 15b Absatzes 1 AsylG-E ist der biometrische Abgleich mit öffentlich zugänglichen Daten aus dem Internet zum Zweck der Feststellung der Identität oder der Staatsangehörigkeit vorzunehmen. Die

Identität umfasst dabei nicht nur den Namen der Person, sondern weitere Merkmale die einen Menschen von anderen Menschen unterscheidet und damit zu einer individuellen Persönlichkeit macht. Zur Identität zählen daher auch Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität der Person sind. Um die Identitätsmerkmale des asylsuchenden Ausländers zu erfassen, ist das BAMF zudem zum Zwecke der Ausführung des Asylgesetzes berechtigt weitere personenbezogene Daten zu erheben. Zur Identität im asylrechtlichen Sinne zählen daher auch das Geburtsland, das Land des gewöhnlichen Aufenthalts, der Familienstand, die Volks- und Religionszugehörigkeit sowie die Sprachkenntnisse des Ausländers.

Unter einem biometrischen Abgleich im Sinne der Vorschrift ist die technisch gestützte Überprüfung der Übereinstimmung von biometrischen Lichtbildern mit dem Ergebnis einer Übereinstimmungsbewertung zu verstehen. Ausgangspunkt ist das vom Ausländer nach § 16 Absatz 1 Satz 1 aufgenommene Lichtbild, das mit Referenzdaten abgeglichen wird. Unter allgemein öffentlich zugängliche Daten fallen solche Daten, die von jedermann verwendet werden können, beispielsweise aus sozialen Medien, soweit sich diese nicht an einen spezifisch abgegrenzten Personenkreis richten. Konkretisierend fallen darunter Daten, wenn sie jede Person ohne oder nach vorheriger Registrierung, Genehmigung oder Entgeltzahlung nutzen kann. Nicht umfasst sind Daten, die einer spezifischen Schwelle unterzogen sind, beispielsweise der Einstellung von Daten in sozialen Medien für einen begrenzten Kreis, dessen Zugang einer Kontrolle unterzogen wird. Privatkommunikation über Messenger-Dienste von sozialen Medien können nicht von der Maßnahme erfasst werden.

Die Befugnis ist technik- und produktneutral. Die Umsetzung kann mittels eigener IT-Produkte der Bundesbehörden oder kommerzieller IT-Produkte Dritter erfolgen.

Die Vorgaben des Artikels 14 der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (ABl. L vom 12.7.2024) (Verordnung über künstliche Intelligenz) sowie des Artikels 22 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119 vom 4.5.2013) (Datenschutz-Grundverordnung) sind zu beachten.

Demnach ist der automatisierte Vorgang vor jeglichen weiteren Maßnahmen oder Entscheidungen durch zwei Personen zu überprüfen und zu bestätigen. Zweifel an der Richtigkeit der Treffer gehen nicht zu Lasten des Ausländers. Aufzeichnungen über Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch den Abgleich erlangt werden, sind unverzüglich zu löschen und die Tatsache ihrer Erlangung und Löschung aktenkundig zu machen. Alle übrigen ausgelesenen Daten sind unverzüglich zu löschen, sobald sie für die Feststellung der Identität oder Staatsangehörigkeit nicht mehr erforderlich sind. Das BAMF hat das Auslesen, Auswerten und Löschen von Daten zur Nachvollziehbarkeit der Maßnahme in der Asylakte zu dokumentieren. Das BAMF hat die betroffene Person über den Zweck, den Umfang und die Durchführung des biometrischen Abgleichs in verständlicher Weise zu informieren.

Zur Durchführung des biometrischen Internetabgleichs nach Absatz 1 kann eine Übermittlung an andere öffentliche oder nichtöffentliche Stellen erforderlich sein. § 15b Absatz 4 AsylG-E sieht insofern eine spezielle Übermittlungsbefugnis vor.

§ 15b AsylG-E ergänzt die Möglichkeiten der Feststellung der Identität und der Staatsangehörigkeit um den automatisierten Abgleich des behördlich erhobenen biometrischen Lichtbilds mit öffentlich zugänglichen Internetdaten. Anders als § 15a AsylG, der ebenfalls zum Zweck der Feststellung der Identität und Staatsangehörigkeit auf das Auslesen und

Auswerten persönlicher Datenträger des Ausländers gerichtet ist, betrifft § 15b ausschließlich den Zugriff auf externe, frei zugängliche Quellen und vermeidet damit Eingriffe in private Datenbestände. Die Norm schafft ein eigenständiges, technisch anders gelagertes Instrument, das die Identitäts- und Staatsangehörigkeitsklärung unterstützt. Für die Anwendung der Befugnisse nach §§ 15a und 15b bedarf es jeweils einer eigenständigen Prüfung der Erforderlichkeit und Verhältnismäßigkeit. Im Vergleich zu § 15a AsylG handelt es sich bei der Maßnahme nach § 15b AsylG-E regelmäßig um das mildere Mittel, da auf öffentlich zugängliche Daten zugegriffen wird.

Zu Nummer 2

Zu Artikel 4 (Inkrafttreten)

Die Bestimmung regelt das Inkrafttreten des Gesetzes.